1183

UNIVERSITE de PARIS - SUD

CENTRE d'ORSAY

THESES

présentées pour obtenir le grade de

DOCTEUR ES-SCIENCES MATHEMATIQUES

par

Pierre KAPLAN

1ère Thèse : "SUR LE 2-GROUPE DES CLASSES D'IDEAUX DES CORPS QUADRATIQUES

2ème Thèse : PROPOSITIONS DONNEES PAR LA FACULTE

SOUTENUE LE 19 novembre 1973 DEVANT LA COMMISSION D'EXAMEN

Messieurs J.P. Kahane Président

J. Poitou Rapporteur

J.J. Payan

1183

UNIVERSITE de PARIS - SUD

CENTRE d'ORSAY

THESES

présentées pour obtenir le grade de

DOCTEUR ES-SCIENCES MATHEMATIQUES

par

Pierre KAPLAN

1ère Thèse : "SUR LE 2-GROUPE DES CLASSES D'IDEAUX DES CORPS QUADRATIQUES

2ème Thèse : PROPOSITIONS DONNEES PAR LA FACULTE

SOUTENUE LE 19 novembre 1973 DEVANT LA COMMISSION D'EXAMEN

Messieurs J.P. Kahane Président
G. Poitou Rapporteur
J.J. Payan

UNIV.
LEIDEN
BIBL.

SUR LE 2-GROUPE DES CLASSES D'IDEAUX DES CORPS QUADRATIQUES

Introduction.

Soit (C_2^*) le 2-groupe des classes d'idéaux au sens étroit de $\mathbb{Q}(\sqrt{D})$, où D est un entier sans diviseur carré. Dans ce travail, nous obtenons de nombreux résultats nouveaux mettant en relation l'existence de cycles d'ordre au moins 8 dans (C_2^*) avec d'autres propriétés de D. Voici trois exemples de ces résultats ; $C(m)$ désigne un groupe cyclique d'ordre m et $C(\geqslant 2^n)$ un groupe cyclique d'ordre 2^k où $k \geqslant n$.

a) Cas $D = 3p$, où $p \equiv 1 \pmod 4$ est un nombre premier.
$(C_2^*) = C(\geqslant 4).C(2)$ si, et seulement si, $p \equiv 1 \pmod{24}$. Sinon $(C_2^*) = C(2)^2$.

Si $p \equiv 1 \pmod{24}$, $p = u^2 + 2v^2 = x^2 + 3y^2$. Alors :
$(C_2^*) = C(\geqslant 8).C(2)$ si, et seulement si, $u + v \equiv \pm 1$ et $x \equiv \pm 1 \pmod{12}$.

b) Cas $D = -2pq$ où p et q sont des nombres premiers tels que

$$p \equiv -q \equiv 1 \pmod 8 \quad \text{et} \quad \left(\frac{p}{q}\right) = -1 .$$

$(C_2^*) = C(\geqslant 8).C(2)$ si, et seulement si, $p + q \equiv 0 \pmod{16}$. Sinon $(C_2^*) = C(4).C(2)$.

c) Cas de $D = 2P$ où P est le produit de n nombres premiers $p \equiv 1 \pmod 8$ non résidus quadratiques les uns des autres et où n est égal à 2 ou à un nombre impair. Le nombre P se décompose sous les formes :

$$P = a^2 + b^2 = u^2 + 2v^2 \text{ , avec } b \equiv 2v \equiv 0 \pmod 4 .$$

Alors, indépendamment du choix des nombres a, b, u et v :
$(C_2^*) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $a \equiv \pm 1$ et $b \equiv 0 \pmod 8$, ou bien encore, si, et seulement si, $u \equiv \pm 1$ et $2v \equiv 0 \pmod 8$. Sinon $(C_2^*) = C(4).C(2)^{n-1}$.

Si $D > 0$, outre des résultats de ce type, nous obtenons simultanément de nombreux résultats nouveaux concernant la résolubilité des équations "non-pelliennes" $x^2 - Dy^2 = d$ où $d \neq 1$ est un diviseur de D si $D \not\equiv -1 \pmod 4$, de $2D$ si $D \equiv -1 \pmod 4$.

Les cas étudiés ici comprennent tous ceux où (C_2^*) est produit de deux groupes cycliques et nous retrouvons, comme cas particuliers, les résultats de notre travail précédent [11] où sont traités les cas où (C_2^*) est cyclique.

La méthode de démonstration utilise uniquement la théorie des formes quadratiques binaires.

§ 1.- Notations, rappels, position et histoire du problème.

Nous noterons p , p' , p'' , $p_1 \dots p_n$ des nombres premiers congrus à 1 modulo 4 et q , q' , q'' , $q_1 \dots q_n$ des nombres premiers congrus à -1 modulo 4 .

Nous désignerons par D un entier rationnel donné qui n'a pas de diviseur carré.

Une forme quadratique binaire $\varphi = AX^2 + 2BXY + CY^2$ sera notée $[A,B,C]$. Nous appellerons déterminant de la forme $\varphi = [A,B,C]$ le nombre $B^2 - AC$, c'est-à-dire l'opposé du déterminant de la matrice $\begin{pmatrix} A & B \\ B & C \end{pmatrix}$ de la forme φ . (cette convention, qui est celle de Gauss ([8]) et Dirichlet ([6] et [7]), permet d'associer au corps $\mathbb{Q}(\sqrt{D})$ des formes de déterminant D) . Nous ne considérons que des formes proprement primitives, où A , B et C sont entiers rationnels et où le P. G. C. D. de A , $2B$ et C est 1 . Deux formes φ et φ' sont équivalentes (noté : $\varphi \sim \varphi'$) si l'on passe de l'une à l'autre par une substitution linéaire à coefficients entiers de déterminant +1 .

Les classes d'équivalence des formes de déterminant D , positives si $D < 0$, forment un groupe (C) pour la composition : deux classes K et K' étant données, il existe des formes $\varphi = [A,B,A'C]$ et $\varphi' = [A',B,AC]$ telles que φ appartienne à K et φ' à K' ; la classe L de $\Psi = [AA',B,C]$, qui est déterminée par K et K' , est dite composée ou produit de K et de K' et est notée KK' ; toute forme de la classe KK' est dite composée, ou produit, de toute forme de K et de toute forme de K' .

Nous désignerons toujours par f la forme $[1,0,-D] = X^2 - DY^2$, par $\mathcal{J}$ sa classe, qui est la classe unité du groupe (C) . Nous noterons $h(D)$ l'ordre du groupe (C) .

Le groupe (C^*) des classes d'idéaux au sens étroit de $\mathbb{Q}(\sqrt{D})$ est isomorphe au groupe (C) ou au quotient de (C) par un sous-groupe à trois éléments, donc leurs 2-composantes (C_2) et (C_2^*) sont isomorphes. (cf. [10], pages 210-217, [7], pages 397-402 et l'appendice à la fin de ce travail).

Pour étudier le groupe (C_2^*) , nous étudierons le groupe isomorphe (C_2) .

Le 2^n-rang d'un 2-groupe G est le nombre de cycles $C(\geqslant 2^n)$ dans toute décomposition de G en produit de groupes cycliques. Notre but étant de déterminer le 8-rang r_8 du groupe (C_2) dans certains cas, rappelons comment on détermine ses 2-rang et 4-rang.

a) Détermination du 2-rang r_2 de (C_2) . Classes ambiguës.

Les classes ambiguës sont les classes de (C) dont le carré est la classe unité $\mathcal{J}$. Depuis Gauss, on sait en trouver des représentants et les compter : appelons "ambiguë simple" une forme du type $[A,0,C]$ avec $|A| < |C|$, ou bien du type $[2B,B,E]$ avec $D = -BB'$ et $|B| < |2E-B| = B'$. Il n'y a de formes du deuxième type que si $D \equiv -1 \pmod 4$. Alors :

Proposition 0 (Gauss).- Les classes ambiguës sont les classes contenant des formes ambiguës simples. Une classe indéfinie ($D > 0$) contient exactement deux formes ambiguës simples ; une classe définie ($D < 0$) en contient exactement une.

Posons $\Delta = 2|D|$ si $D \equiv -1 \pmod 4$ et $\Delta = |D|$ sinon (Δ est le produit des nombres premiers ramifiés dans $Q(\sqrt{D})$) . Soit δ le nombre des facteurs premiers de Δ ; la proposition 0 montre que $r_2 = \delta - 1$. En particulier :

(C_2) est réduit à H si $D = -1$, ± 2 , p , $-q$.

(C_2) est cyclique si $\delta = 2$, donc $D = -p$, q , $\pm 2p$, $\pm 2q$, pp' , qq' , $-pq$, (cf. [11]).

(C_2) est produit de deux groupes cycliques si $\delta = 3$, donc :

$$D = pp'p'' , pqq' , 2pp' , 2pq , 2qq' , pq \quad (D > 0)$$
$$D = -pp'q , -qq'q'' , -pp' , -qq' , -2pp' , -2pq , -2qq' \quad (D < 0) .$$

La proposition 0 montre que toute classe ambiguë représente des diviseurs de Δ . On prouve que, réciproquement, toute classe qui représente un diviseur de Δ est une classe ambiguë.

La forme f est toujours ambiguë simple. Si $D > 0$, le problème de déterminer comment se groupent deux par deux les formes ambiguës simples dans chaque classe ambiguë revient à trouver la deuxième forme ambiguë simple équivalente à f , c'est-à-dire à déterminer les deux diviseurs propres de Δ représentés par f ; ces diviseurs sont les facteurs principaux. En particulier, l'équation $t^2 - Du^2 = -1$ a des solutions si, et seulement si, $f \overset{N}{\sim} \bar{f} = [-1,0,D]$, ou encore si, et seulement si, -1 est facteur principal.

b) Détermination du 4-rang r_4 de (C_2) . Genres.

Soit d un diviseur premier de Δ . Si d est impair, tous les nombres m premiers à d représentés par une même forme φ de déterminant $-D$ donnent la même valeur $e_d(\varphi)$ au symbole de Legendre $(\frac{m}{d})$; de même, si $d = 2$ (alors $D \not\equiv 1 \pmod 4$) , tous les nombres impairs m représentés par une même forme φ de déterminant $-D$ donnent la même valeur $e_2(\varphi)$ à la fonction suivante :

$$(\tfrac{-1}{m}) = (-1)^{\frac{m-1}{2}} \text{ si } D \equiv -1 \pmod 4 \; ; \; (-1)^{\frac{m^2-1}{8}} = (\tfrac{2}{m}) \text{ si } D \equiv 2 \pmod 8$$
$$(-1)^{\frac{m^2-1}{8} + \frac{m-1}{2}} = (\tfrac{-2}{m}) \text{ si } D \equiv 6 \pmod 8 .$$

Les nombres $e_d(\varphi)$ sont les caractères génériques de la forme φ , ou, puisque deux formes équivalentes représentent les mêmes nombres, les caractères génériques de la classe K de φ ; nous les noterons aussi $e_d(K)$. Si M désigne le produit de certains des nombres d , nous poserons :

$$e_M(\varphi) = \prod_{d|M} e_d(\varphi) .$$

Comme D est quadrat-frei, le produit des valeurs de tous les caractères génériques pour chaque forme vaut 1. C'est ce résultat, conséquence de la Loi de Réciprocité quadratique, que nous appelerons "formule du produit" :

A partir du paragraphe 4, il sera souvent commode de noter les caractères génériques de la manière suivante : si d est un diviseur premier impair de Δ, au lieu de $e_d(\varphi)$, on écrira $(\frac{m}{d})$, ce qui signifie "la valeur du symbole de Legendre $(\frac{m}{d})$ pour tout nombre m premier à d représenté par φ". De même, suivant le cas, au lieu de $e_2(\varphi)$, on écrira $(\frac{-1}{m})$, $(\frac{2}{m})$, $(\frac{-2}{m})$, ou bien

$$(-1)^{\frac{m-1}{2}}, \quad (-1)^{\frac{m^2-1}{8}}, \quad (-1)^{\frac{m^2-1}{8}+\frac{m-1}{2}}.$$

Deux classes sont dans le même genre si elles donnent la même valeur à tous les caractères génériques. Une classe est dans le genre principla si tous ses caractères valent 1. La composition induit une loi de groupe sur l'ensemble des genres, loi pour laquelle le genre principal est l'unité. Le résultat fondamental de la théorie des genres est :

Théorème 0 (Gauss).- Les classes du genre principal sont le sous-groupe des carrés de (C) ; le groupe (C) contient $2^{\delta-1}$ genres donnant aux caractères génériques toutes les valeurs compatibles avec la formule du produit.

Soit r_4 le 4-rang de (C). Le nombre des classes ambiguës qui sont des carrés est 2^{r_4}, donc, tenant compte de la proposition 0 et du théorème 0, on obtient :

Théorème A_0.-

1) Le nombre des formes ambiguës simples qui sont dans le genre principal est 2^{r_4} si $D<0$, 2^{r_4+1} si $D>0$.

2) Quand $D>0$, $r_4=0$ si, et seulement si, la forme $f=[1,0,-D]$ est la seule forme ambiguë simple du genre principal de déterminant $-D$.

3) Quand D 0, $r_4=0$ si, et seulement si, il y a exactement deux formes ambiguës simples dans le genre principal, f et une autre g qui est équivalente à f. Alors deux formes ambiguës simples du même genre sont équivalentes et les facteurs principaux sont les diviseurs de Δ donnant la valeur 1 à tous les caractères génériques.

4) Les genres des classes ambiguës constituent un sous-groupe d'indice 2^{r_4} du groupe des genres.

Pour appliquer le théorème A_0 à l'étude de r_4 et des facteurs principaux si $D>0$ et $r_4=0$, nous ferons la liste des formes ambiguës simples et examinerons lesquelles sont dans le genre principal. Nous désignerons par "propositions A" les résultats obtenus ainsi.

Comme le théorème A_0, les propositions A, même si elles n'ont pas été formulées auparavant, sont des conséquences immédiates des résultats de Gauss.

c) Détermination du 8-rang r_8 de $(\ )_2$.

Le nombre 2^{r_8} est le nombre des classes ambiguës dont une des racines carrées est dans le genre principal. Donc :

Théorème BC_0.-

1) Le nombre des formes ambiguës simples dont une des racines carrées est dans le genre principal est 2^{r_8} si $D<0$, 2^{r_8+1} si $D>0$.

2) Quand $D<0$, $r_8=0$ si, et seulement si, la forme $f=[1,0,-D]$ est la seule forme ambiguë simple qui ait une racine carrée dans le genre principal.

3) Quand $D>0$, $r_8=0$ si, et seulement si, il y a exactement deux formes ambiguës simples, f et une autre g , dont une des racines carrées soit dans le genre principal. Ces formes f et g sont équivalentes.

Pour appliquer ce théorème BC_0, nous devons comparer les genres des classes ambiguës avec le genre d'une des racines carrées de chaque forme ambiguë simple du genre principal.

Nous le ferons d'une part si $r_4=1$, avec $r_2=1$ ou 2 et dans certains cas où $r_2>2$ et, d'autre part, si $r_2=r_4=2$.

α) Méthode pour les cas où $r_4=1$.

Si $r_4=1$, le théorème A_0, 4) montre que les genres des classes ambiguës constituent un sous-groupe d'indice 2 du groupe des genres, sous-groupe formé de tous les genres vérifiant une relation $e_\nu=1$, où ν est un diviseur de Δ (autre que 1 et Δ) que nous déterminerons pour chaque type de D envisagé. Si la forme g est dans le genre principal, le nombre $e_\nu(\sqrt{g})$ a la même valeur pour toutes les racines carrées de g .

Si $D<0$, il y a exactement deux formes ambiguës simples dans le genre principal, f et une autre h . Désignant par $\sqrt{h}$ une quelconque des racines carrées de h , on voit que $r_8=1$ si, et seulement si, $e_\nu(\sqrt{h})=1$.

Si $D>0$, il y a quatre formes ambiguës simples dans le genre principal, f , h_1 , h_2 et h_3 . Si h_i est équivalente à f , e_ν vaut 1 pour toute racine carrée de h_i et à la même valeur pour les racines carrées des deux autres formes h qui sont équivalentes. Donc, quel que soit le choix des racines carrées :

$$e_\nu(\sqrt{h_1}).e_\nu(\sqrt{h_2}).e_\nu(\sqrt{h_3})=1 .$$

En outre, $r_8=1$ si, et seulement si, h_1 , h_2 et h_3 sont des puissances quatrièmes, donc si, et seulement si, $e_\nu(\sqrt{h_1})=e_\nu(\sqrt{h_2})=e_\nu(\sqrt{h_3})=1$. Sinon $r_8=0$ et la forme h_i équivalente à f est celle telle que $e_\nu(\sqrt{h_i})=1$.

Nous appelerons méthode B ce raisonnement et nous désignerons les résultats obtenus ainsi par théorèmes B et propositions B si $D > 0$, par propositions B' si $D < 0$.

β) Méthode pour les cas où $r_2 = r_4 = 2$.

Si $r_2 = r_4 = 2$, toutes les classes ambiguës sont dans le genre principal, car $2^{r_2} = 2^{r_4}$. Nous utiliserons le théorème BC_0 , en tenant compte de cette simplification.

Nous désignerons les résultats obtenus ainsi par propositions C si $D > 0$, par propositions C' si $D < 0$.

γ) Genre de racines carrées de formes ambiguës simples.

C'est le point le plus difficile de la théorie. Nous utilisons deux méthodes, suivant le type du nombre D .

La première méthode consiste, quand c'est possible, à exprimer le caractère e_D d'une racine carrée de la forme ambiguë simple du genre principal $[D',0,-D'']$ par le symbole biquadratique rationnel $(\frac{D''}{D'})_4$ (lemmes 1 à 3).

La deuxième méthode consiste à déterminer explicitement des racines carrées de formes ambiguës simples du genre principal. Le plus simple de ces résultats (lemme 4), combiné avec les lemmes 1 à 3 permet de prouver facilement, au début du paragraphe 3, ce dont nous avons besoin à propos de la réciprocité biquadratique, c'est-à-dire des lois de réciprocité biquadratique rationnelle générale nouvelles. Le reste de ce paragraphe est consacré à l'étude des cas $D = p_1 \dots p_n$, où nous retrouvons les résultats que Scholz [17] et Redei [16] démontraient à partir de la théorie du corps de classe et au cas $D = 2p_1 \dots p_n$, où nous trouvons des résultats nouveaux, bien plus simples que ceux de [16]. Au paragraphe 4, nous appliquons les résultats précédents à l'étude complète des cas $D = pp'p''$ et $D = 2pp'$. Dans les paragraphes 5 à 10, nous étudions les autres cas où $r_2 = 2$ et certains cas où $r_2 > 2$. Les lemmes 1 à 4 ne suffisent pas pour traiter tous les cas et nous devons utiliser d'autres idées, en particulier une méthode de Gauss (DA, § 286) pour trouver effectivement la racine carrée d'une classe du genre principal.

Les paragraphes 11 et 12 sont consacrés à l'étude des corps imaginaires ($D < 0$) . Certains des résultats de ces paragraphes ont été obtenus soit par Redei [16], soit par E. Brown [5].

Le paragraphe 13 contient un résultat concernant le problème, un peu différent, de déterminer quelles classes de déterminant donné représente un nombre premier. Mais la méthode de démonstration est voisine de celle de la théorie qui précède et en utilise un résultat. En outre, les résultats de ce paragraphe 13 sont nécessaires pour étudier le 16-rang r_{16} de (C_2) dans certains cas (cf. [12]).

d) Remarques sur l'histoire de ces problèmes.

Les premiers résultats concernant ces questions remontent à Gauss et à Legendre, vers 1800. Gauss applique la proposition 0 au cas $D = p \equiv 1 \pmod 4$ pour prouver que $t^2 - pu^2 = -1$ est résoluble ; Legendre démontre ce résultat par une autre méthode. En utilisant la méthode de Legendre et des cas particuliers de nos lemmes 1 à 3, Dirichlet, en 1834 ([6], p. 219), obtient les premiers résultats concernant les équations non pelliennes $t^2 - pp'u^2 = -1$ et $t^2 - 2p''u^2 = -1$ dans des cas où les caractères génériques ne suffisent pas à décider de leur résolubilité : $(\frac{p}{p'}) = 1$ et $p'' \equiv 1 \pmod 8$; mais il ne remarque pas le lien de cette question avec le problème de la structure de (C_2), ni Tano [20] qui généralise ces résultats.

C'est presque un siècle après Dirichlet que Scholz ([14]) et Redei ([13]), guidés par la théorie du corps de classes, remarquent ce lien. Scholz se limite au cas où $D = p_1 \dots p_n$, tandis que Redei étudie aussi d'autres cas ; en revanche, en utilisant la proposition 0, ([14], p. 99), Scholz obtient des résultats concernant les équations non pelliennes autres que $x^2 - Dy^2 = -1$. Ainsi, pour le cas $D = pp'$, $(\frac{p}{p'}) = 1$:

α) $(C_2) = C(\geqslant 8)$ si $(\frac{p'}{p})_4 = (\frac{p}{p'})_4 = 1$. Sinon $(C_2) = C(4)$.

β) Si $(\frac{p'}{p})_4 = -(\frac{p}{p'})_4 = 1$, $t^2 - pp'u^2 = p$ a des solutions.

γ) Si $(\frac{p'}{p})_4 = (\frac{p}{p'})_4 = -1$, $t^2 - pp'u^2 = -1$ a des solutions.

Dirichlet prouve γ), Redei prouve α) et γ) et Scholz : α), β) et γ).

Vers 1968-1970, G. Pall ([15]) et E. Brown ([2] et [4]) ont étudié la résolubilité des équations non pelliennes dans certains cas $(D = 2p , 5p , 13p , 3p)$.

Ils partent aussi de la proposition 0 et utilisent les algèbres de quaternions. Leurs résultats sont des cas particuliers des nôtres.

Simultanément, plusieurs auteurs ont obtenu, dans certains cas où (C_2) est cyclique et $D < 0$, des critères pour que (C_2) soit cyclique d'ordre au moins 8 ; leurs théories sont résumées dans [11], où leurs travaux sont cités. Elles sont généralisées dans ce travail, en particulier au paragraphe 12. D'ailleurs, parmi ces résultats, celui concernant $\mathbb{Q}(\sqrt{-p})$ où $p = a^2 + b^2 \equiv 1 \pmod 8$, à savoir : "$(C_2) = C(\geqslant 8)$ si, et seulement si, $a + b \equiv \pm 1 \pmod 8$" avait été communiqué par Gauss à Dirichlet dans une lettre du 30 mai 1828.

En 1972, G. Gras ([9]) a découvert une méthode générale pour étudier le ℓ-groupe des classes des extensions cycliques de degré premier ℓ. Appliquée aux corps quadratiques, cette méthode permet d'arriver à certains de nos résultats, ceux qui peuvent être obtenus sans utiliser les "méthodes de Dirichlet et Gauss" des paragraphes 2 et 8.

§ 2.- Genres de racines carrées de formes ambiguës simples.

Rappelons que D désigne un entier quadrat-frei donné et que nous considérons le groupe (C) des classes de formes de déterminant D .

a) Usage du symbole biquadratique rationnel.

Rappelons la définition du symbole biquadratique rationnel :

Soit $p \equiv 1 \pmod 4$ et a tel que $\left(\frac{a}{p}\right) = 1$. $\left(\frac{a}{p}\right)_4$ est égal à 1 ou -1 , suivant que a est ou non résidu biquadratique de p . Autrement dit :

Si $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, alors $\left(\frac{a}{p}\right)_4 \equiv a^{\frac{p-1}{4}} \pmod p$.

En particulier $\left(\frac{-1}{p}\right)_4 = (-1)^{\frac{p-1}{4}}$.

Il sera commode d'utiliser le symbole $\left(\frac{a}{2}\right)_4$ défini pour $a \equiv 1 \pmod 8$: $\left(\frac{a}{2}\right)_4 = 1$ si $a \equiv 1 \pmod{16}$, $\left(\frac{a}{2}\right)_4 = -1$ si $a \equiv 9 \pmod{16}$.

Le symbole dont le dénominateur est composé est défini multiplicativement.

Nous avons défini le symbole $\left(\frac{A}{P}\right)_4$ quand $P = 2^{\beta} \prod_{i=1}^{n} p_i$, $\left(\frac{A}{p_i}\right) = 1$ $(i = 1 , \ldots , n)$ et $A \equiv 1 \pmod 8$ si $\beta > 0$. Quand ces conditions sont réalisées, nous dirons par définition : le symbole $\left(\frac{A}{P}\right)_4$ est défini.

Les lemmes 1, 2 et 3 généralisent des raisonnements de Dirichlet.

Lemme 1.- Soit $D = PP'$ où P est le produit de nombres premiers congrus à 1 modulo 4 et P' un entier rationnel congru à 1 modulo 4 . Si $g = [P, 0, -P']$ est dans le genre principal, les caractères génériques de toute racine carrée φ de g vérifient :

$$e_P(\varphi) = \left(\frac{P'}{P}\right)_4 .$$

Soit m un entier premier à 2D représenté par une racine carrée φ de g . m^2 est représenté par g , donc :

$$m^2 = Px^2 - P'y^2 . \qquad (1)$$

Dans cette relation, x est premier à P' et y premier à P . Un carré impair étant congru à 1 modulo 8 , (1) entraîne d'abord :

$$1 \equiv x^2 - y^2 \pmod 4 .$$

Donc x est impair et y pair. Posons $y = 2^h z$ où z est impair et $h > 0$: l'équation (1) entraîne :

$$P - 1 \equiv 2^{2h} P' z^2 \pmod 8 .$$

Donc $h = 1$ si $P \equiv 5 \pmod 8$.

Soient p_i $(i = 1 \ldots n)$ les facteurs premiers de P . Calculons $\left(\frac{m}{p_i}\right)$:

$$\left(\frac{m}{p_i}\right) = \left(\frac{-P'y^2}{p_i}\right)_4 = (-1)^{\frac{p_i-1}{4}} \left(\frac{P'}{p_i}\right)_4 \left(\frac{z}{p_i}\right) \left(\frac{2}{p_i}\right)^h = \left(\frac{P'}{p_i}\right)_4 \left(\frac{p_i}{z}\right) \left(\frac{2}{p_i}\right)^{h+1} .$$

Comme h ne dépend pas de i et que $h + 1 = 2$ si le nombre des p_i tels que $\left(\frac{2}{p_i}\right) = -1$ est impair, on trouve en multipliant :

$$\left(\frac{m}{P}\right) = \left(\frac{P'}{P}\right)_4 \left(\frac{P}{z}\right) .$$

Mais $\left(\frac{P}{z}\right) = \left(\frac{Px^2}{z}\right) = \left(\frac{m^2}{z}\right) = 1$, car $m^2 \equiv Px^2 \pmod z$ C. Q. F. D.

Lemme 2.- Soit $D = 2PP'$ où P est le produit de nombres premiers P_i congrus à 1 modulo 4 et où P' est congru à 1 modulo 4 et premier à P . Si $g = [P,0,-P']$ est dans le genre principal, alors $P' \equiv 1 \pmod 8$ et les caractères génériques de toute racine carrée φ de g vérifient :

$$e_{2P}(\varphi) = \left(\frac{P'}{2P}\right)_4 .$$

Comme g est dans le genre principal $e_2(g) = \left(\frac{2}{P'}\right) = 1$, donc $P' \equiv 1 \pmod 8$.

Soit m un entier premier à D représenté par φ . On a :

$$e_{2P}(\varphi) = \left(\frac{2}{m}\right) \left(\frac{m}{P}\right) \quad \text{et :} \quad (2) \qquad m^2 = 2Px^2 - P'y^2 .$$

Calculons $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$. L'équation (2) montre que y est impair, donc $2Px^2 \equiv 2 \pmod 8$, donc x est impair, donc $2x^2 \equiv 2 \pmod{16}$ et :

$$\frac{m^2-1}{8} = \frac{2Px^2-2}{8} - \frac{P'y^2-1}{8} \equiv \frac{P-1}{4} + \frac{P'y^2-1}{8} \equiv \frac{P-1}{4} + \frac{P'-1}{8} + \frac{y^2-1}{8} \pmod 2 .$$

La dernière congruence venant de l'identité $ab - 1 = a - 1 + b - 1 + (a-1)(b-1)$. Donc :

$$\left(\frac{2}{m}\right) = \left(\frac{2}{P}\right) \left(\frac{P'}{2}\right)_4 \left(\frac{2}{y}\right) .$$

La démonstration du lemme 1 avec y à la place de z et $h = 0$ montre que :

$$\left(\frac{m}{p_i}\right) = \left(\frac{2}{p_i}\right) \left(\frac{P'}{P}\right)_4 \left(\frac{p_i}{y}\right) .$$

Multipliant, il vient, puisque $2Px^2 \equiv m^2 \pmod y$:

$$\left(\frac{2}{m}\right) \left(\frac{m}{P}\right) = \left(\frac{P'}{2P}\right)_4 \left(\frac{2P}{y}\right) = \left(\frac{P'}{2P}\right)_4 \quad \text{C. Q. F. D.}$$

Lemme 3.- Soit $D = PQ$, où P est produit de nombres premiers congrus à 1 modulo 8 et Q un entier rationnel premier à P . Si $g = [P,0,-Q]$ est dans le genre principal, les caractères de toute racine carrée φ de g vérifient :

$$e_P(\varphi) = \left(\frac{Q}{P}\right)_4 .$$

La démonstration est semblable à celle du lemme 1 ; comme les p_i sont congrus à 1 (mod 8) , la parité de y dans l'équation $m^2 = Px^2 - Qy^2$ n'intervient pas.

Les lemmes 1 et 2 suffisent pour retrouver les résultats de Dirichlet ([6], pages 219-236) et Tano ([20]) concernant la résolubilité de $t^2 - Du^2 = -1$:

Si $t^2 - Du^2 = -1$ a des solutions, $D = 2^\alpha \prod_i p_i$ où $\alpha = 0$ ou 1. En outre, toute forme $g = [D',0,-D'']$ est équivalente à $\bar{g} = [D'',0,-D']$.

Si $\left(\frac{D'}{D''}\right)_4$ et $\left(\frac{D''}{D'}\right)_4$ sont définis, g est dans le genre principal, donc g et $\bar{g}$ sont les carrés d'une même forme h et on a $\left(\frac{D'}{D''}\right)_4 = e_{D''}(h)$ et $\left(\frac{D''}{D'}\right)_4 = e_{D'}(h)$, donc $\left(\frac{D'}{D''}\right)_4 = \left(\frac{D''}{D'}\right)_4$ par la formule du produit. Donc nous avons prouvé le

Corollaire 1.- Si $t^2 - Du^2 = -1$ a des solutions, il n'existe pas de décomposition $D = D'D''$ telles que $\left(\frac{D'}{D''}\right)_4$ et $\left(\frac{D''}{D'}\right)_4$ soient définis et différents.

Corollaire 2.- Soit $D = 2^\alpha \prod_i p_i$ où $\alpha = 0$ ou 1. Si pour toutes les décompositions $D = D'D''$ autres que $D = 1.D$ et $D = D.1$ telles que $\left(\frac{D'}{D''}\right)_4$ et $\left(\frac{D'}{D''}\right)_4$ soient définis on a $\left(\frac{D'}{D''}\right)_4 = \left(\frac{D''}{D'}\right)_4 = -1$, alors $t^2 - Du^2 = -1$ a des solutions.

Sinon, il existerait une forme $g = [D',0,-D'']$ équivalente à f, où $D' > 1$. $\left(\frac{D'}{D''}\right)_4$ et $\left(\frac{D''}{D'}\right)_4$ seraient définis et $\left(\frac{D''}{D'}\right)_4$ serait égal à 1.

b) Calculs explicites de racines carrées de formes ambiguës simples.

Lemme 4.- Si $D = A^2 + B^2$, avec A premier à $2B$, alors $[A,B,-A]$ est une racine carrée de $[-1,0,D]$.

La démonstration du lemme 4 est immédiate, en composant $[A,B,-A]$ avec elle-même.

La théorie des formes indéfinies réduites permet de préciser ce résultat :

Lemme 4'.- Les racines carrées de la classe de $[-1,0,D]$ sont les classes contenant des formes du type $[A,B,-A]$ et chaque classe en contient exactement deux : un couple $[A,B,-A]$, $[-A,B,A]$ si $[-1,0,D] \sim [1,0,-D]$, un couple $[A,B,-A]$, $[A',B',-A']$ avec $|A'| \neq |A|$ si $[-1,0,D] \sim [1,0,-D]$.

Pour la démonstration, voir [13], chapitre VIII.

Dans les lemmes suivants, on désigne par M et N deux entiers rationnels dont le produit est $-D$ et tels que M soit impair si $N \equiv 1 \pmod 4$. On suppose que la forme $g = [M,0,N]$ est dans le genre principal de déterminant D et on cherche à en déterminer explicitement une racine carrée.

Lemme 5.- Si la forme $g = [M,0,N]$ est dans le genre principal de déterminant D, M est représenté par une forme du genre principal de déterminant N.

En effet, N est résidu quadratique de tous les facteurs premiers de M et est impair si M est pair. La congruence $X^2 \equiv N \pmod{M}$ a donc des solutions, donc M est représenté par des formes φ de déterminant N, formes qui sont bien proprement primitives, car M est impair si $N \equiv 1 \pmod{4}$. M est résidu quadratique de tous les facteurs premiers de N, donc tous les caractères génériques de φ, sauf éventuellement $e_2(\varphi)$, valent 1, donc la formule du produit pour φ montre que $e_2(\varphi) = 1$. C. Q. F. D.

Lemme 6.- Si $M = X^2 - NY^2$ avec X impair, alors la forme $[X,NY,NX]$ est une racine carrée de la forme $[M,0,N]$.

En effet, la forme $[X,NY,NX]$ est proprement primitive, a pour déterminant D et pour carré la forme $[X^2,NY,N]$ équivalente à $[M,0,N]$.

Le lemme 4 est le cas particulier du lemme 6 où $M = D$, $N = -1$.

Remarque : Dans l'égalité $M = X^2 - NY^2$, X ne peut être pair que si $D \equiv 1 \pmod{4}$.

En effet, si X est pair, $M \equiv -NY^2 \pmod{4}$; comme $M \not\equiv 0 \pmod{4}$, Y est impair, donc $M \equiv -N \pmod{4}$, donc $D = -MN \equiv +1 \pmod{4}$.

En combinant les lemmes 5 et 6 et la remarque, on obtient :

Lemme 7.- Si la forme $[M,0,N]$ est dans le genre principal de déterminant D et si un genre de déterminant N ne contient qu'une classe, alors $M = X^2 - NY^2$. Si X est impair, ce qui est toujours le cas si $D \not\equiv 1 \pmod{4}$, une racine carrée de $[M,0,N]$ est $[X,NY,NX]$.

Le lemme 7 permettra d'obtenir des résultats dans de nombreux cas particuliers où D se décompose sous la forme $D = -MN$ de telle manière qu'il y ait une seule classe dans un genre de déterminant N.

Au paragraphe 8, nous étudierons le cas général où il y a plusieurs classes dans un genre de déterminant N.

§ 3.- Cas où D est positif et n'a pas de diviseur premier $q \equiv -1 \pmod 4$.

(D $p_1 \dots p_n$ et $D = 2p_1 \dots p_n$)

Dans ces cas, deux formes $\varphi = [a,b,c]$ et $\bar{\varphi} = [-a,b,-c]$ sont toujours dans le même genre. D est somme de deux carrés et nous poserons $D = A^2 + B^2$, où A est impair.

a) Réciprocité biquadratique rationnelle.

Proposition 1.-

α) Cas $D = p_1 \dots p_n$.

Si la forme $g = [P,0,-P']$ est dans le genre principal de déterminant D , les caractères de toute classe ambiguë $\mathfrak{A}$ vérifient $e_P(\mathfrak{A}) = e_{P'}(\mathfrak{A}) = 1$.

β) Cas $D = 2p_1 \dots p_n$.

Si la forme $h = [2P,0,-P']$ est dans le genre principal de déterminant D , alors $P' \equiv 1 \pmod 8$ et les caractères de toute classe ambiguë $\mathfrak{A}$ vérifient $e_{2P}(\mathfrak{A}) = e_{P'}(\mathfrak{A}) = 1$.

Cette proposition est une conséquence de la Loi de Réciprocité quadratique : la formule du produit pour $\mathfrak{A}$ montre qu'il suffit de vérifier une des deux relations. Vérifions par exemple $e_{P'}(\mathfrak{A}) = 1$ dans le cas β) :

Soit $h = [\pm 2P_1 P_2', 0, \mp P_2 P_1']$ une forme ambiguë simple, où $P_1 P_2 = P$ et $P_1' P_2' = P'$. Pour h , on trouve

$$e_{P'}(h) = \left(\frac{2P_1 P_2'}{P_1'}\right)\left(\frac{P_2 P_1'}{P_2'}\right) = \left(\frac{2P_1}{P_1'}\right)\left(\frac{P_2}{P_2'}\right)\left(\frac{P_2'}{P_1'}\right)\left(\frac{P_1'}{P_2'}\right) = \left(\frac{2P_1}{P_1'}\right)\left(\frac{P_2}{P_2'}\right) .$$

Comme g est dans le genre principal $\left(\frac{2P_1 P_2}{P_1'}\right) = 1$, donc $e_{P'}(h) = \left(\frac{P_2}{P'}\right) = \left(\frac{P'}{P_2}\right) = 1$.

Théorème 1 (Loi de Réciprocité biquadratique rationnelle générale).-

Soient P et P' deux nombres quadrat-frei premiers entre eux, dont tous les facteurs premiers sont congrus à 1 modulo 4 .

1) Si les symboles $\left(\frac{P}{P'}\right)_4$ et $\left(\frac{P'}{P}\right)_4$ sont définis, soit $PP' = A^2 + B^2$, A impair. Alors :

$$\left(\frac{P}{P'}\right)_4 \cdot \left(\frac{P'}{P}\right)_4 = \left(\frac{A}{P}\right) = \left(\frac{A}{P'}\right) .$$

2) Si les symboles $\left(\frac{2P'}{P}\right)_4$ et $\left(\frac{P}{2P'}\right)_4$ sont définis, soit $2PP' = A^2 + B^2$. Alors :

$$\left(\frac{A}{P'}\right)\left(\frac{2}{A}\right) = \left(\frac{A}{P}\right) = \left(\frac{2P'}{P}\right)_4 \left(\frac{P'}{2P}\right)_4 .$$

Démontrons par exemple 1). L'hypothèse "$\left(\frac{P'}{P}\right)_4$ et $\left(\frac{P}{P'}\right)_4$ sont définis" signifie exactement que $g = [P,0,-P']$ et $\bar{g} = [P',0,-P]$ sont dans le genre principal de déterminant $D = PP'$. Soit $\bar{f} = [-1,0,D]$. On a $\bar{g} \approx \bar{f}\, g$ et la même relation est vraie pour leurs racines carrées modulo une classe ambiguë, dont les caractères génériques vérifient $e_P = e_{P'} = 1$. Mais d'après les lemmes 1 et 4,

$e_P = e_{P'}$ vaut $(\frac{P}{P'})_4$, $(\frac{P'}{P})_4$, $(\frac{A}{P})$ pour une racine carrée de $\bar{g}$, g et $\bar{f}$ respectivement. C. Q. F. D.

Cas particuliers :

1) Appliquons le théorème 1, a) au cas où P et P' sont des nombres premiers $p = a^2 + b^2$ et $p' = a'^2 + b'^2$ (a et a' impairs) tels que $(\frac{p}{p'}) = 1$.

Comme $pp' = (aa'+bb')^2 + (ab'-a'b)^2$, on trouve la formule :

$$(\frac{p}{p'})_4 (\frac{p'}{p})_4 = (\frac{aa'+bb'}{p}) = (\frac{aa'+bb'}{p'}) .$$

2) Appliquons le théorème 1, b) au cas où $P' = 1$. Tous les facteurs premiers de P sont congrus à 1 modulo 8 et l'on a :

$P = a^2 + b^2 = u^2 + 2v^2 = 2e^2 - d^2 = e'^2 - 2d'^2$ ($b \equiv 0 \pmod 4$, e et $e' > 0$) .

Comme $2P = (a+b)^2 + (a-b)^2$, le théorème 1, b) se traduit ici par :

$$(\frac{2}{a+b}) = (\frac{a+b}{P}) = (\frac{2}{P})_4 (\frac{P}{2})_4 .$$

On a $(\frac{2}{a+b}) = (\frac{2}{a}) (-1)^{\frac{b}{4}}$ et, comme $P \equiv a^2 \pmod{16}$, $(\frac{P}{2})_4 = (\frac{2}{a})$, donc :

$$(\frac{2}{P})_4 = (-1)^{\frac{b}{4}} .$$

Les équations $2P = 2u^2 + 4v^2 = 4e^2 - 2d^2$ montrent que $[u,2v,-2u]$ et $[d,2e,2d]$ sont racines carrées de $\bar{g} = [-2,0,P]$ et $g = [2,0,-P]$ respectivement. Donc (lemmes 1 et 3) on a : $(\frac{2}{u}) = (\frac{2}{P})_4$ et $(\frac{2}{d}) = (\frac{P}{2})_4$.

En outre, $\frac{v}{2}$ est pair si, et seulement si, $P \equiv u^2 \pmod{16}$, donc, puisque $P \equiv a^2 \pmod{16}$, si, et seulement si, $(\frac{2}{a}) = (\frac{2}{u})$, c'est-à-dire si, et seulement si, $(\frac{2}{a}) = (-1)^{\frac{b}{4}}$. Donc $(-1)^{\frac{v}{2}} = (\frac{2}{a+b})$.

Enfin, $P = 2e^2 - d^2$ montre que $(\frac{2}{P})_4 (\frac{e}{P}) = (\frac{d}{P})$ et la formule du produit pour $[e,d,2e]$ est : $(\frac{e}{P}) = (\frac{-1}{e})$. De même, $(\frac{e'}{P}) = (\frac{2}{P})_4 (\frac{d'}{P}) = (\frac{2}{P})_4 (\frac{P}{d''}) = (\frac{2}{P})_4$, où d" désigne la partie impaire de d' .

En résumé, nous avons démontré le :

Théorème 2.- Soit P un produit de nombres premiers distincts congrus à 1 modulo 8 et soient $P = a^2 = b^2 = u^2 + 2v^2 = 2e^2 - d^2 = e'^2 - 2d'^2$ (a impair) des décompositions de P . Indépendamment du choix de a , b , u , v , e , d , e' , d' , on a :

$$(\frac{P}{2})_4 = (\frac{2}{a}) = (\frac{2}{d}) \quad ; \quad (\frac{2}{P})_4 = (-1)^{\frac{b}{4}} = (\frac{2}{u}) = (\frac{e'}{P}) = (\frac{-2}{|e'|})$$

$$(\frac{P}{2})_4 (\frac{2}{P})_4 = (\frac{2}{a+b}) = (\frac{a+b}{P}) = (-1)^{\frac{v}{2}} = (\frac{e}{P}) = (\frac{-1}{|e|}) .$$

Nous poserons : $\lambda(P) = (\frac{2}{a+b})$; $\mu(P) = (\frac{2}{a})$; $\nu(P) = (-1)^{\frac{b}{4}}$. On a donc :

$\lambda(P).\mu(P).\gamma(P) = 1$.

On peut, par décompositions successives, démontrer le théorème 1 à partir des lois "simples" que sont le cas particulier 1 et le théorème 2 pour $P = p$ premier, mais c'est plus compliqué que de procéder directement.

Ces cas simples étaient déjà connus, mais les théorèmes 1 et 2 ne semblent pas avoir été formulés auparavant sous leur forme générale. Notre démonstration des théorèmes 1 et 2 est entièrement nouvelle ; une première version pour le cas particulier 1 se trouve dans notre travail précédent [11].

b) Etude du cas où $r_4 = 1$.

Supposons $r_4 = 1$ et désignons par D' et D'' les deux entiers bien déterminés tels que les quatre formes ambiguës simples du genre principal soient : $f = [1,0,-D]$, $\bar{f} = [-1,0,D]$, $g = [D',0,-D'']$, $[-D',0,D'']$ et $\bar{g} = [D'',0,-D']$.

La proposition 1 montre que les genres des classes ambiguës sont ceux qui vérifient $e_{D'} = e_{D''} = 1$, c'est-à-dire que $V = D'$ ou D'' .

Les lemmes 1 et 2 montrent que les caractères génériques des racines carrées de g et $\bar{g}$ vérifient respectivement :

$$e_{D'}(\sqrt{g}) = \left(\frac{D''}{D'}\right)_4 \; ; \; e_{D'}(\sqrt{\bar{g}}) = e_{D''}(\sqrt{\bar{g}}) = \left(\frac{D'}{D''}\right)_4 .$$

Donc on obtient par la méthode B :

Théorème B_1.- Soit D un entier positif sans facteur premier $q \equiv -1 \pmod 4$ et tel qu'il existe une seule décomposition $D = D'D''$ autre que $1.D$ telle que $\left(\frac{D'}{D''}\right)_4$ et $\left(\frac{D''}{D'}\right)_4$ soient définis. Alors :

a) Pour que $(C_2)(D) = C(\geqslant 8).C(2)^{n-1}$, il faut et il suffit que $\left(\frac{D'}{D''}\right)_4 = \left(\frac{D''}{D'}\right)_4 = 1$. Sinon $(C_2)(D) = C(4).C(2)^{n-1}$.

b) Si $\left(\frac{D'}{D''}\right)_4 = \left(\frac{D''}{D'}\right)_4 = -1$, f représente -1 .

c) Si $\left(\frac{D'}{D''}\right)_4 = 1$, $\left(\frac{D''}{D'}\right)_4 = -1$, f représente D'' .

d) Si $\left(\frac{D'}{D''}\right)_4 = -1$, $\left(\frac{D''}{D'}\right)_4 = 1$, f représente D' .

Les hypothèses du théorème B_1 sont vérifiées en particulier dans les cas suivants :

1) Proposition B_1.- Soit $D = p_o p_1 \ldots p_n = p_o P$ où $n = 2$ ou un nombre impair, $\left(\frac{p_i}{p_o}\right) = 1$, $\left(\frac{p_i}{p_j}\right) = -1$ pour $0 \leqslant i < j \leqslant n$.

Alors $(C_2) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $\left(\frac{p_o}{P}\right)_4 = \left(\frac{P}{p_o}\right)_4 = 1$. Sinon $(C_2) = C(4).C(2)^{n-1}$ et :

Si $\left(\frac{p_o}{P}\right)_4 = \pm 1$ et $\left(\frac{P}{p_o}\right)_4 = \mp 1$, f représente $\mp p_o$.

Si $\left(\frac{p_o}{P}\right)_4 = \left(\frac{P}{p_o}\right)_4 = -1$, f représente -1 .

En effet, on voit que les seules formes ambiguës simples du genre principal sont f , $\bar{f} = [-1,0,D]$, $g = [p_o,0,-P]$, $\bar{g} = [-p_o,0,P]$.

2) Proposition B_2.- Soit $D = 2p_1 \dots p_n$ où n est 2 ou un nombre impair, $p_i \equiv 1 \pmod 8$ et $(\frac{p_i}{p_j}) = -1$ pour $1 \leqslant i < j \leqslant n$. Posons $p_1 \dots p_n = P$.

$(C_2) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $\lambda(P) = \mu(P) = \nu(P) = 1$. Sinon $(C_2) = C(4).C(2)^{n-1}$ et un seul des $\lambda(P)$, $\mu(P)$, $\nu(P)$ vaut 1 . La forme $f = [1,0,-D]$ représente -1 , 2 , -2 suivant que $\lambda(P) = 1$, $\mu(P) = 1$, $\nu(P) = 1$.

En effet, les formes ambiguës simples du genre principal sont :
$f = [1,0,-D]$, $\bar{f} = [-1,0,D]$, $g = [2,0,-P]$, $\bar{g} = [-2,0,P]$.

Ceci montre que $r_4 = 1$ et $V = 2$. D'autre part, le caractère e_2 vaut $\lambda(P)$, $\mu(P)$, $\nu(P)$ pour des racines carrées de $\bar{f}$, g et $\bar{g}$ respectivement.

Corollaire B_2.- Soit $D = 2p_1 \dots p_n$ où $p_i \equiv 1 \pmod 8$ et $(\frac{p_i}{p_j}) = -1$; $n = 1$, 2 ou impair, $p_1 \dots p_n = P = a^2 + b^2$.

1) $(C_2) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $a \equiv \pm 1$ et $b \equiv 0 \pmod 8$. Sinon $C_2 = C(4).C(2)^{n-1}$.

2) Si $a \equiv \pm 1$ et $b \equiv 4 \pmod 8$, $[1,0,-D]$ représente 2 .
Si $a \equiv \pm 3$ et $b \equiv 0 \pmod 8$, $[1,0,-D]$ représente -2 .
Si $a \equiv \pm 3$ et $b \equiv 4 \pmod 8$, $[1,0,-D]$ représente -1 .

Tenant compte des formules pour $\lambda(P)$, $\mu(P)$, $\nu(P)$, on obtient d'autres critères, car on voit que :

$a \equiv \pm 1$ et $b \equiv 0 \pmod 8 \Longleftrightarrow |e| \equiv 1 \pmod 4$ et $d \equiv \pm 1 \pmod 8 \Longleftrightarrow u \equiv \pm 1$ et $2v \equiv 0 \pmod 8$
$a \equiv \pm 1$ et $b \equiv 4 \pmod 8 \Longleftrightarrow |e| \equiv 3 \pmod 4$ et $d \equiv \pm 1 \pmod 8 \Longleftrightarrow u \equiv \pm 3$ et $2v \equiv 4 \pmod 8$
$a \equiv \pm 3$ et $b \equiv 0 \pmod 8 \Longrightarrow |e| \equiv 3 \pmod 4$ et $d \equiv \pm 3 \pmod 8 \Longleftrightarrow u \equiv \pm 1$ et $2v \equiv 4 \pmod 8$
$a \equiv \pm 3$ et $b \equiv 4 \pmod 8 \Longleftrightarrow |e| \equiv 1 \pmod 4$ et $d \equiv \pm 3 \pmod 8 \Longleftrightarrow u \equiv \pm 3$ et $2v \equiv 0 \pmod 8$

§ 4.- Etude complète des cas $D = pp'p''$ et $2pp'$.

a) Cas de $D = pp'p''$ où $p \equiv p' \equiv p'' \equiv 1 \pmod 4$. $D = A^2 + B^2$ avec A impair.

Les caractères génériques sont $(\frac{m}{p})$, $(\frac{m}{p'})$, $(\frac{m}{p''})$ et (C_2) est produit de deux groupes cycliques. Les formes ambiguës simples sont équivalentes à :

$f = [1,0,-pp'p'']$, $g = [p,0,-p'p'']$, $g' = [p',0,-pp'']$, $g'' = [p'',0,-pp']$
$\bar{f} = [-1,0,pp'p'']$, $\bar{g} = [-p,0,p'p'']$, $\bar{g}' = [-p',0,pp'']$, $\bar{g}'' = [-p'',0,pp']$.

f et $\bar{f}$, g et $\bar{g}$, g' et $\bar{g}'$, g'' et $\bar{g}''$ sont dans le même genre.
Posons : $\varepsilon = (\frac{p'}{p''}) = (\frac{p''}{p'})$; $\varepsilon' = (\frac{p}{p''}) = (\frac{p''}{p})$; $\varepsilon'' = (\frac{p}{p'}) = (\frac{p'}{p})$.

Le tableau des valeurs des caractères pour les formes ambiguës est :

	f et $\bar{f}$	g et $\bar{g}$	g' et $\bar{g}'$	g'' et $\bar{g}''$
$(\frac{m}{p})$	1	$\varepsilon'\varepsilon''$	ε''	ε'
$(\frac{m}{p'})$	1	ε'	$\varepsilon\varepsilon''$	ε
$(\frac{m}{p''})$	1	ε''	ε	$\varepsilon\varepsilon'$

Proposition A_1.- Si deux ou trois des ε valent -1 , seules f et $\bar{f}$ sont dans le genre principal, la seule classe ambiguë qui soit un carré est la classe unité de f et $\bar{f}$ et :

1) (C_2) est de type $C(2)^2$.

2) L'équation $t^2 - Du^2 = -1$ a des solutions.

3) $f \sim \bar{f}$, $g \sim \bar{g}$, $g' \sim \bar{g}'$, $g'' \sim \bar{g}''$.

a_1) Si $\varepsilon = -1$, $\varepsilon' = \varepsilon'' = 1$. Posons : $\alpha = (\frac{p'p''}{p})_4$ et $\beta = (\frac{p}{p'p''})_4$.
Le tableau des caractères est ici :

	f et $\bar{f}$	g et $\bar{g}$	g' et $\bar{g}'$	g'' et $\bar{g}''$
$(\frac{m}{p})$	1	1	1	1
$(\frac{m}{p'})$	1	1	-1	-1
$(\frac{m}{p''})$	1	1	-1	-1

La théorie du § 3 donne :

Proposition B .-

1) $(\frac{A}{p})$ ne dépend pas du choix de A et $(\frac{A}{p}) = \alpha\beta$.

2) Pour que $(C_2) = C(\geq 8).C(2)$, il faut et il suffit que $\alpha = \beta = 1$ (ou que $\alpha = (\frac{A}{p}) = 1$, ou que $\beta = (\frac{A}{p}) = 1$) . Sinon $(C_2) = C(4).C(2)$.

3) Si $\alpha = \beta = -1$: f représente -1 .
Si $\alpha = \pm 1$, $\beta = \mp 1$: f représente $\mp p$.

a_2) Si $\varepsilon = \varepsilon' = \varepsilon'' = 1$. Posons : $\alpha = \left(\frac{p'p''}{p}\right)_4$, $\alpha' = \left(\frac{pp''}{p'}\right)_4$, $\alpha'' = \left(\frac{pp'}{p''}\right)_4$, $\beta = \left(\frac{p}{p'p''}\right)_4$, $\beta' = \left(\frac{p'}{pp''}\right)_4$, $\beta'' = \left(\frac{p''}{pp'}\right)_4$.

(C_2) contient $C(4).C(4)$, les quatre classes ambiguës sont dans le genre principal et le tableau des caractères de leurs racines carrées est :

	$\sqrt{f}$	$\sqrt{\bar{f}}$	$\sqrt{g}$	$\sqrt{\bar{g}}$	$\sqrt{g'}$	$\sqrt{\bar{g}'}$	$\sqrt{g''}$	$\sqrt{\bar{g}''}$
$\left(\frac{m}{p}\right)$	1	$\left(\frac{A}{p}\right)$	α	β				
$\left(\frac{m}{p'}\right)$	1	$\left(\frac{A}{p'}\right)$			α'	β'		
$\left(\frac{m}{p''}\right)$	1	$\left(\frac{A}{p''}\right)$					α''	β''

α) Si (C_2) contient $C(8) \times C(8)$, toutes ces formes sont des carrés, donc

$$\alpha = \beta = \alpha' = \beta' = \alpha'' = \beta'' = \left(\frac{A}{p}\right) = \left(\frac{A}{p'}\right) = \left(\frac{A}{p''}\right) = 1 .$$

β) Si $t^2 - Du^2 = -1$ a des solutions, c'est-à-dire si $f \sim \bar{f}$, alors $g \sim \bar{g}$, $g' \sim \bar{g}'$, $g'' \sim \bar{g}''$.

On en déduit d'abord que $\left(\frac{A}{p}\right) = \left(\frac{A}{p'}\right) = \left(\frac{A}{p''}\right) = 1$, $\alpha = \beta$, $\alpha' = \beta'$, $\alpha'' = \beta''$ et le tableau des caractères devient :

	$\sqrt{f}$	$\sqrt{g}$	$\sqrt{g'}$	$\sqrt{g''}$
$\left(\frac{m}{p}\right)$	1	α	η'	η''
$\left(\frac{m}{p'}\right)$	1	η_1	α'	η_1''
$\left(\frac{m}{p''}\right)$	1	η_2	η_2'	α''

Les η valent 1 ou -1 . Le produit des termes d'une colonne vaut 1 (formule du produit) et, comme $g'g'' \sim g$, $\sqrt{g'}\sqrt{g''} \sim \sqrt{g}$ modulo une classe ambiguë, ce qui montre que le produit des termes d'une ligne vaut 1 .

Si $\alpha = \alpha' = \alpha'' = 1$, on trouve $\eta' = \eta'' = \eta_1'' = \eta_1 = \eta_2 = \eta_2' = \pm 1$ et (C_2) contient $C(8).C(8)$ ou est $C(4).C(4)$ suivant que le signe est + ou - .

Si $\alpha = -1$, $\alpha' = \alpha'' = 1$, on trouve toujours $\sqrt{g'}$ ou bien $\sqrt{g''}$ dans le genre principal, donc $(C_2) = C(\geqslant 8).C(4)$.

Si $\alpha = 1$, $\alpha' = \alpha'' = -1$, on trouve, suivant le signe des η , que $(C_2) = C(4).C(4)$ ou $C(\geqslant 8).C(4)$ $(n \geqslant 3)$.

Si $\alpha = \alpha' = \alpha'' = -1$, $C(2) = C(4).C(4)$.

γ) Si $t^2 - Du^2 = p$ a des solutions, c'est-à-dire si $f \sim g$, alors $\bar{f} \sim \bar{g}$, $g' \sim \bar{g}''$, $g'' \sim \bar{g}'$ et le tableau des caractères des racines carrées devient :

	$\sqrt{f}$	$\sqrt{\bar{f}}$	$\sqrt{g'}$	$\sqrt{\bar{g}''}$
$\left(\frac{m}{p}\right)$	$1 = \alpha$	$\left(\frac{A}{p}\right) = \beta$	$\alpha'\beta''$	$\alpha'\beta''$
$\left(\frac{m}{p'}\right)$	1	$\left(\frac{A}{p'}\right) = \alpha'\beta'$	α'	β'
$\left(\frac{m}{p''}\right)$	1	$\left(\frac{A}{p''}\right) = \alpha''\beta''$	α''	β''

Dans les cas où $t^2 - Du^2 = -1$ n'a pas de solutions, on voit que si $\alpha' = \alpha'' = \beta' = \beta'' = 1$, alors $\alpha = \beta = (\frac{A}{p}) = (\frac{A}{p'}) = (\frac{A}{p''}) = 1$ et que (C_2) contient $C(8).C(8)$.

Résumons :

Proposition C_1.- Soient $pp'p''$ trois nombres premiers congrus à 1 modulo 4 tels que $(\frac{p}{p'}) = (\frac{p'}{p''}) = (\frac{p''}{p}) = 1$. Posons $\alpha = (\frac{p'p''}{p})_4$, $\alpha' = (\frac{pp''}{p'})_4$, $\alpha'' = (\frac{pp'}{p''})_4$, $\beta = (\frac{p}{p'p''})_4$, $\beta' = (\frac{p'}{pp''})_4$, $\beta'' = (\frac{p''}{pp'})_4$. Soit $D = pp'p'' = A^2 + B^2$ (A impair).

a) $(\frac{A}{p}) = \alpha\beta$, $(\frac{A}{p'}) = \alpha'\beta'$, $(\frac{A}{p''}) = \alpha''\beta''$ et $\alpha\beta\alpha'\beta'\alpha''\beta'' = 1$.

b) (C_2) contient un sous-groupe $C(4) \times C(4)$. Si (C_2) contient un sous-groupe $C(8) \times C(8)$, alors $\alpha = \alpha' = \alpha'' = \beta = \beta' = \beta'' = 1$.

c) Si $t^2 - Du^2 = -1$ n'a pas de solutions et si $\alpha' = \alpha'' = \beta' = \beta'' = 1$, alors (C_2) contient un sous-groupe $C(8) \times C(8)$ et $\alpha = \beta = 1$.

d) Si $t^2 - Du^2 = -1$ a des solutions : $\alpha = \beta$, $\alpha' = \beta'$, $\alpha'' = \beta''$.
Si $t^2 - Du^2 = p$ a des solutions : $\alpha = 1$.
Si $t^2 - Du^2 = -p$ a des solutions : $\beta = 1$.

Corollaire.- Si $\alpha = \alpha' = \alpha'' = \beta = \beta' = \beta'' = -1$, $t^2 - Du^2$ représente -1 .

b) Cas de $D = 2pp'$.

Les caractères génériques sont : $(\frac{m}{p})$, $(\frac{m}{p'})$, $(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$.

Les formes ambiguës simples sont équivalentes à :

$$f = [1,0,-2pp'] \ , \ g = [2,0,-pp'] \ , \ h = [p,0,-2p'] \ , \ h' = [p',0,-2p]$$
$$\bar{f} = [-1,0,2pp'] \ , \ \bar{g} = [-2,0,pp'] \ , \ \bar{h} = [-p,0,2p'] \ , \ \bar{h}' = [-p',0,2p] \ .$$

Posons $(\frac{2}{p}) = \varepsilon$, $(\frac{2}{p'}) = \varepsilon'$, $(\frac{p}{p'}) = (\frac{p'}{p}) = \varepsilon''$. Le tableau des caractères est :

	f et $\bar{f}$	g et $\bar{g}$	h et $\bar{h}$	h' et $\bar{h}'$
$(\frac{m}{p})$	1	ε	$\varepsilon\varepsilon''$	ε''
$(\frac{m}{p'})$	1	ε'	ε''	$\varepsilon'\varepsilon''$
$(\frac{2}{m})$	1	$\varepsilon\varepsilon'$	ε	ε'

Proposition A_2.- Si deux des ε , ε' , ε'' valent -1 , seules f et $\bar{f}$ sont dans le genre principal, donc -1 est facteur principal, $(C_2) = C(2)^2$ et $g \overset{N}{\sim} \bar{g}$, $h \overset{N}{\sim} \bar{h}$ et $h' \overset{N}{\sim} \bar{h}'$.

1) Si $\varepsilon = \varepsilon' = 1$, $\varepsilon'' = -1$, c'est-à-dire si $p \equiv p' \equiv 1 \pmod 8$ et $(\frac{p}{p'}) = -1$.

Le genre principal contient f , $\bar{f}$, g et $\bar{g}$. Les caractères des classes ambiguës sont 1 , 1 , 1 et -1 , -1 , 1 . Le corollaire 2 (§ 3) donne le résultat, en posant $pp' = a^2 + b^2 = u^2 + 2v^2 = 2a^2 - d^2$.

2) Si $\varepsilon = \varepsilon'' = 1$, $\varepsilon' = -1$, c'est-à-dire si $p \equiv 1$, $p' \equiv 5 \pmod 8$, $\left(\frac{p}{p'}\right) = 1$, $p = a_1^2 + b_1^2$. Le genre principal contient f , $\bar{f}$, h et $\bar{h}$. Les caractères des classes ambiguës sont 1 , 1 , 1 et 1 , -1 , -1 . On obtient

<u>Proposition</u> B_2.- $(C_2) = C(\geqslant 8).C(2)$ <u>si, et seulement si,</u> $\left(\frac{2p'}{p}\right)_4 = \left(\frac{p}{2p'}\right)_4 = 1$.

<u>Si</u> $\left(\frac{2p'}{p}\right)_4 = 1$, $\left(\frac{p}{2p'}\right)_4 = -1$, f <u>représente</u> p <u>et</u> $-2p'$.

<u>Si</u> $\left(\frac{2p'}{p}\right)_4 = -1$, $\left(\frac{p}{2p'}\right)_4 = 1$, f <u>représente</u> $-p$ <u>et</u> $2p'$.

<u>Si</u> $\left(\frac{2p'}{p}\right)_4 = \left(\frac{p}{2p'}\right)_4 = -1$, f <u>représente</u> -1 .

3) Si $\varepsilon' = \varepsilon'' = \varepsilon = 1$, c'est-à-dire si $p \equiv p' \equiv 1 \pmod 8$ et $\left(\frac{p}{p'}\right) = 1$.

Posons $pp' = a^2 + b^2 = u^2 + 2v^2 = 2e^2 - d^2$. Toutes les classes ambiguës sont dans le genre principal, donc (C_2) contient $C(4).C(4)$. Le tableau des caractères des racines carrées des classes ambiguës est :

	$\sqrt{f}$	$\sqrt{\bar{f}}$	$\sqrt{g}$	$\sqrt{\bar{g}}$	$\sqrt{h}$	$\sqrt{\bar{h}}$	$\sqrt{h'}$	$\sqrt{\bar{h}'}$
$\left(\frac{m}{p}\right)$	1	$\left(\frac{a+b}{p}\right)$	$\left(\frac{d}{p}\right)$	$\left(\frac{u}{p}\right)$	$\left(\frac{2p'}{p}\right)_4$			$\left(\frac{p'}{2p}\right)_4$
$\left(\frac{m}{p'}\right)$	1	$\left(\frac{a+b}{p'}\right)$	$\left(\frac{d}{p'}\right)$	$\left(\frac{u}{p'}\right)$		$\left(\frac{p}{2p'}\right)_4$	$\left(\frac{2p}{p'}\right)_4$	
$\left(\frac{2}{m}\right)$	1	$\left(\frac{2}{a+b}\right) = (-1)^{\frac{v}{2}}$	$\left(\frac{2}{d}\right) = \left(\frac{2}{a}\right)$	$\left(\frac{2}{u}\right) = (-1)^{\frac{b}{4}}$				

Parmi les résultats que l'on peut déduire de ce tableau, mentionnons :

<u>Proposition</u> C_2.- <u>Si</u> $\left(\frac{d}{p}\right) = \left(\frac{d}{p'}\right) = \left(\frac{u}{p}\right) = \left(\frac{u}{p'}\right) = \left(\frac{2p'}{p}\right)_4 = \left(\frac{p}{2p'}\right)_4 = \left(\frac{2p}{p'}\right)_4 = \left(\frac{p'}{2p}\right)_4 = 1$, <u>alors</u> (C_2) <u>contient</u> $C(8)^2$.

En effet, quelle que soit la manière dont se groupent les formes ambiguës simples, il y a au moins une colonne de 1 dans le tableau des caractères des racines carrées. Il y en a deux, sauf dans le cas où $f \approx g$, $h \approx \bar{h}'$ et $\bar{h} \approx h'$. Alors le tableau est :

$$\begin{matrix} 1 & 1 & \eta_3 \\ 1 & \eta_1 & 1 \\ 1 & \eta_2 & \eta_4 \end{matrix}$$

d'où $\eta_1 = \eta_2 = \eta_3 = \eta_4 = 1$ C. Q. F. D.

§ 5.- Cas où $D = pq$ $(p \equiv -q \equiv 1 \pmod 4)$.

a) Les caractères génériques sont $(\frac{m}{p})$, $(\frac{m}{q})$ et $(-1)^{\frac{m-1}{2}}$. Il y a quatre genres, quatre classes ambiguës, $r_4 = 1$ et les formes ambiguës simples sont équivalentes à :

$$f = [1,0,-pq] \text{ , } g = [p,0,-q] \text{ , } h = [2,1,\tfrac{1-pq}{2}] \text{ , } k = [2p,p,\tfrac{p-q}{2}]$$

$$\bar{f} = [-1,0,pq] \text{ , } \bar{g} = [q,0,-p] \text{ , } \bar{h} = [-2,1,\tfrac{pq-1}{2}] \text{ , } \bar{k} = [2q,q,\tfrac{q-p}{2}] .$$

Posons $(\frac{p}{q}) = (\frac{q}{p}) = \varepsilon$, $(\frac{2}{p}) = \varepsilon'$, $(\frac{2}{q}) = \varepsilon''$. La valeur des caractères pour ces formes est :

	f	$\bar{f}$	g	$\bar{g}$	h	$\bar{h}$	k	$\bar{k}$
$(\frac{m}{p})$	1	1	ε	ε	ε'	ε'	$\varepsilon\varepsilon'$	$\varepsilon\varepsilon'$
$(\frac{m}{q})$	1	-1	ε	$-\varepsilon$	ε''	ε''	$\varepsilon\varepsilon''$	$-\varepsilon\varepsilon''$
$(-1)^{\frac{m-1}{2}}$	1	-1	1	-1	$\varepsilon'\varepsilon''$	$-\varepsilon'\varepsilon''$	$\varepsilon'\varepsilon''$	$-\varepsilon'\varepsilon''$

Si $\varepsilon = \varepsilon' = -1$: k ou $\bar{k}$ est dans le genre principal suivant que $\varepsilon'' = +1$ ou -1 .

Si $\varepsilon = -1$, $\varepsilon' = 1$: h ou $\bar{h}$ est dans le genre principal suivant que $\varepsilon'' = +1$ ou -1 .

Si $\varepsilon = 1$, $\varepsilon' = -1$: g est dans le genre principal.

Ainsi, dans les cas où ε ou ε' vaut -1 , il y a deux formes ambiguës simples par genre, donc $r_4 = 0$ et :

Proposition A_3.- Si $p \equiv 5 \pmod 8$, ou si $(\frac{p}{q}) = -1$, (C_2) est du type $C(2).C(2)$. L'équivalence des formes ambiguës simples et les facteurs principaux sont déterminés par les caractères génériques.

b) A partir d'ici, on suppose $\varepsilon = \varepsilon' = 1$, c'est-à-dire $(\frac{p}{q}) = 1$ et $p \equiv 1 \pmod 8$.

Le tableau des caractères des formes ambiguës simples est :

	f	$\bar{f}$	g	$\bar{g}$	h	$\bar{h}$	k	$\bar{k}$
$(\frac{m}{p})$	1	1	1	1	1	1	1	1
$(\frac{m}{q})$	1	-1	1	-1	ε''	$-\varepsilon''$	ε''	$-\varepsilon''$
$(-1)^{\frac{m-1}{2}}$	1	-1	1	-1	ε''	$-\varepsilon''$	ε''	$-\varepsilon''$

Donc si $\varepsilon'' = 1$ $(q \equiv -1 \pmod 8)$, le genre principal contient f , g , h et k et si $\varepsilon'' = -1$ $(q \equiv 3 \pmod 8)$, le genre principal contient f , g , $\bar{h}$ et $\bar{k}$. Donc exactement deux des classes ambiguës sont dans le genre principal, donc $r_4 = 1$. On voit d'autre part que $V = p$.

D'après le lemme 3, la valeur du caractère générique $e_V = (\frac{m}{p})$ de toute racine carrée de g est $(\frac{q}{p})_4$.

b_1) Cas où $q \equiv 3 \pmod 8$. $\varepsilon'' = -1$.

Ici, le genre principal contient f , g , $\bar{h}$ et $\bar{k}$. D'autre part :

$$p = u^2 + 2v^2 \ , \ q = w^2 + 2z^2 \ , \ pq = (uw \mp 2vz)^2 + 2(uz \pm vw)^2 \ .$$

Posons $pq = B^2 + 2C^2$. Chaque forme $\psi = [C,B,-2C]$ a pour carré $\bar{h}$. On a donc $e_V(\bar{h}) = \left(\frac{uz+vw}{p}\right)$ et on obtient par la méthode B :

Théorème B_2.- Soit $D = pq$ où $p \equiv 1$, $q \equiv 3 \pmod 8$ et $\left(\frac{p}{q}\right) = 1$. Alors $p = u^2 + 2v^2$ et $q = w^2 + 2z^2$; $\left(\frac{uz+vw}{p}\right)$ ne dépend pas des signes de u , v , w , z . En outre :

a) $(C_2) = C(2^3).C(2)$ si, et seulement si, $\left(\frac{uz+vw}{p}\right) = \left(\frac{q}{p}\right)_4 = 1$. Sinon $(C_2) = C(4).C(2)$.

b) Si $\left(\frac{uz+vw}{p}\right) = -1$, $\left(\frac{q}{p}\right)_4 = 1$, f est équivalente à g et représente p et $-q$.

c) Si $\left(\frac{uz+vw}{p}\right) = 1$, $\left(\frac{q}{p}\right)_4 = -1$, f est équivalente à $\bar{h}$ et représente -2 .

d) Si $\left(\frac{uz+vw}{p}\right) = \left(\frac{q}{p}\right)_4 = -1$, f est équivalente à $\bar{k}$ et représente $-2p$ et $2q$

Remarque : $\left(\frac{uz+vw}{p}\right) = \left(\frac{uz+vw}{q}\right)\left(\frac{-1}{uz+vw}\right)$ ("formule du produit" pour ψ) .

Cas particulier de $q = 3$: C'est le seul $q \equiv 3 \pmod 8$ où il y a une seule classe de déterminant $-q$. Ici $w = z = 1$, donc $uz + vw = u + v$.

On voit que $p = x^2 + 3y^2$ et que $[x,3y,-3x]^2 \sim g$ (cf. lemme 6). Donc :

$$\left(\frac{3}{p}\right)_4 = \left(\frac{x}{p}\right) = \left(\frac{x}{3}\right)\left(\frac{-1}{x}\right) \ .$$

Utilisant la remarque et appliquant le théorème B_2, il vient :

Corollaire B_2.- Soit $D = 3p$ où $p \equiv 1 \pmod{24}$; $p = u^2 + 2v^2 = x^2 + 3y^2$.

a) $(C_2) = C(2^3).C(2)$ si, et seulement si, $u + v \equiv \pm 1$ et $x \equiv \pm 1 \pmod{12}$. Sinon $(C_2) = C(4).C(2)$.

b) Si $u + v \equiv \pm 1$ et $x \equiv \pm 5 \pmod{12}$, -2 est facteur principal.

c) Si $u + v \equiv \pm 5$ et $x \equiv \pm 1 \pmod{12}$, -3 est facteur principal.

d) Si $u + v \equiv \pm 5$ et $x \equiv \pm 5 \pmod{12}$, 6 est facteur principal.

Les conditions "$u + v \equiv \pm 1 \pmod{12}$" et "$x \equiv \pm 1 \pmod{12}$" sont respectivement équivalentes à "$\left(\frac{u+v}{p}\right) = 1$" et à "$\left(\frac{x}{p}\right) = 1$" (cf. remarque 1).

Les points b), c), d) du corollaire B_2 sont le résultat essentiel de [4], résultat démontré par une toute autre méthode.

b_2) Cas de $q \equiv -1 \pmod 8$. $\varepsilon = \varepsilon' = \varepsilon'' = 1$.

Le genre principal contient f , g , h , k . En outre, dans ce cas :

$$p = 2e^2 - d^2 = d'^2 - 2e'^2 \quad (e,d,d' \text{ impairs, } e' \text{ pair})$$

$$q = 2r^2 - s^2 = s'^2 - 2r'^2 \quad (s,s',r' \text{ impairs, } r \text{ pair})$$

$$pq = (2er \pm sd)^2 - 2(es \pm dr)^2 = (2e'r' \pm s'd') - 2(e's' \pm d'r')^2 .$$

Posons : $pq = G^2 - 2E^2$. Chaque forme $[E,G,2E]$ a pour discriminant pq , pour carré h , donc ici, on obtient le

Théorème B_3.- Soit $D = pq$ tel que $p \equiv 1$, $q \equiv -1 \pmod 8$ et $\left(\frac{p}{q}\right) = 1$. Alors $p = 2e^2 - d^2$, $q = 2r^2 - s^2$ et $\left(\frac{es+dr}{p}\right) = \left(\frac{e's'+d'r'}{p}\right)$ ne dépend pas du choix de d , e , d' , e' , r , s , r' , s' .

a) $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $\left(\frac{es+dr}{p}\right) = \left(\frac{q}{p}\right)_4 = 1$.

b) Si $\left(\frac{es+dr}{p}\right) = -1$, $\left(\frac{q}{p}\right)_4 = 1$, f est équivalente à g .

c) Si $\left(\frac{es+dr}{p}\right) = 1$, $\left(\frac{q}{p}\right)_4 = -1$, f est équivalente à h .

d) Si $\left(\frac{es+dr}{p}\right) = \left(\frac{q}{p}\right)_4 = -1$, f est équivalente à k .

Cas de $q = 7$: C'est le seul $q \equiv -1 \pmod 8$ tel qu'il y ait une classe de déterminant $-q$. Le lemme 7 montre que $g \approx [x',7y',-7x']^2$ et $\left(\frac{7}{p}\right)_4 = \left(\frac{x'}{p}\right)$. Comme ici $r = 2$ et $s = 1$, posant $e_{14}(m) = \left(\frac{m}{7}\right)\left(\frac{-1}{m}\right)$, on trouve :

Corollaire B_3.- Soit $D = 7p$ tel que $p \equiv 1 \pmod 8$ et $\left(\frac{p}{7}\right) = 1$ ($p \equiv 1$, 9 ou $25 \pmod{56}$) . On a $p = 2e^2 - d^2 = x'^2 + 7y'^2$ et $(C_2) = C(\geqslant 4).C(2)$.

a) $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $e_{14}(e+2d) = e_{14}(x') = 1$.

b) Si $e_{14}(e+2d) = -1$ et $e_{14}(x') = 1$, -7 est facteur principal.

c) Si $e_{14}(e+2d) = 1$ et $e_{14}(x') = -1$, 2 est facteur principal.

d) Si $e_{14}(e+2d) = e_{13}(x') = -1$, -14 est facteur principal.

On a $e_{14}(m) = 1$ pour $m \equiv \pm 1$, ± 3 ou $\pm 9 \pmod{28}$ et $e_{14}(m) = -1$ pour $m \equiv \pm 5$, ± 11 ou $\pm 13 \pmod{28}$. On a aussi $e_{14}(x') = \left(\frac{x'}{p}\right)$ et $e_{14}(e+2d) = \left(\frac{e+2d}{p}\right)$.

Exemples numériques :

a) Tableau des dix plus petits $D = 3p$ tels que $r_8 = 1$.

$p = x^2 + 3y^2 = u^2 + 2v^2$ tel que $x \equiv \pm 1$ et $u + v \equiv \pm 1 \pmod{12}$.

D	p	x	u	v	u + v
1299	433	1	19	6	25
2019	673	25	5	18	13
2811	937	13	17	18	1
3963	1321	11	13	24	37
4971	1657	35	37	12	25
7563	2521	13	37	24	13
11019	3673	59	55	18	37
11307	3769	61	59	12	47
11667	3889	1	19	42	61

b) Tableau des dix plus petits $D = 7p$ tels que $r_8 = 1$.

$p = 2e^2 - d^2 = x'^2 + 7y'^2 = a^2 + b^2$ tel que $(\frac{x'}{p}) = (\frac{x'}{7})\,(\frac{-1}{x'}) = 1$ et $(\frac{e+2d}{p}) = (\frac{e+2d}{7})\,(\frac{-1}{e+2d}) = 1$.

D	p	a	b	x'	e	d	e + 2d
1351	193	7	12	9	11	7	25
6671	953	13	28	29	29	27	25
7063	1009	15	28	1	23	7	9
9023	1289	35	8	29	27	13	1
12607	1801	35	24	3	31	11	9
18599	2657	49	16	17	37	9	19
19607	2801	49	20	1	51	49	47
22799	3257	11	56	53	43	21	1
25151	3593	53	28	59	53	45	37
27503	3929	35	52	59	45	9	27

(L'intérêt d'introduire a et b est que la Loi de Réciprocité biquadratique complexe permet, ici, de remplacer "$(\frac{x'}{p}) = 1$" par "7 divise a ou b" : Notons $((-))$ le symbole biquadratique complexe et soit $a + bi$ un facteur premier complexe de p . Si $(\frac{-7}{p}) = 1$, on a $(\frac{-7}{p})_4 = ((\frac{-7}{a+bi})) = ((\frac{a+bi}{7}))$; or, 0 mis à part, il y a 48 classes complexes modulo 7 et $((\frac{a+bi}{7}))$ vaut 1 pour 12 d'entre elles. Or, on voit que (puisque $48 \equiv 0 \pmod{16}$) , $((\frac{a}{7}))$ et $((\frac{bi}{7})) = 1$, donc les 12 classes tellles que $((\frac{a+bi}{7})) = 1$ sont celles telles que a ou $b \equiv 0 \pmod 7$. Donc si $(\frac{-7}{p}) = 1$ et si 7 ne divise ni a , ni b , $((\frac{a+bi}{7})) = -1$ (cf. [19], pages 242...).

c) $D = pq$ où $q > 7$.

Prenons les plus petits exemples où $(C_2) = C(\geqslant 8).C(2)$.

c_1) $D = 3247 = 17.191$; $p = 17$, $q = 191 \equiv -1 \pmod 8$

$17 = 2.3^1 - 1$, $191 = 2.10^2$, $es + dr = 9 + 10 = 19$

$\left(\frac{es+dr}{p}\right) = \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = 1$; $\left(\frac{191}{17}\right)_4 = \left(\frac{21}{17}\right)_4 = \left(\frac{4}{17}\right)_4 = \left(\frac{2}{17}\right) = 1$.

c_2) $D = 3403 = 41.83$; $p = 41$, $q = 83 \equiv 3 \pmod 8$

$41 = 3^2 + 2.4^2$, $83 = 9^2 + 2$, $uz + vw = 3 + 36 = 39$

$\left(\frac{uz+vw}{p}\right) = \left(\frac{39}{41}\right) = \left(\frac{-2}{41}\right) = 1$; $\left(\frac{83}{41}\right)_4 = \left(\frac{1}{41}\right)_4 = 1$.

§ 6.- Cas de $D = 2pq$ où $p \equiv -q \equiv 1 \pmod 4$.

Les caractères génériques sont $(\frac{m}{p})$, $(\frac{m}{q})$ et $(\frac{-2}{m})$.

Posons $\varepsilon = (\frac{p}{q})$, $\varepsilon' = (\frac{2}{p})$, $\varepsilon'' = (\frac{2}{q})$.

Les formes ambiguës simples sont équivalentes à :

$$f = [1,0,-2pq] \text{ , } g = [p,0,-2q] \text{ , } h = [2,0,-pq] \text{ , } k = [q,0,-2p]$$
$$\bar{f} = [-1,0,2pq] \text{ , } \bar{g} = [-p,0,2q] \text{ , } \bar{h} = [-2,0,pq] \text{ , } \bar{k} = [-q,0,2p] .$$

Le tableau des caractères de ces formes est :

	f	$\bar{f}$	g	$\bar{g}$	h	$\bar{h}$		$\bar{k}$
$(\frac{m}{p})$	1	1	ε'	ε'	$\varepsilon\varepsilon'$	$\varepsilon\varepsilon'$		ε
$(\frac{m}{p'})$	1	-1	ε''	$-\varepsilon''$	ε	$-\varepsilon$	$-\varepsilon\varepsilon''$	$\varepsilon\varepsilon''$
$(\frac{-2}{m})$	1	-1	$\varepsilon'\varepsilon''$	$-\varepsilon'\varepsilon''$	ε'	$-\varepsilon'$	$-\varepsilon''$	ε''

a) On vérifie, comme pour le cas où $D = pq$, que, si ε ou ε' vaut -1 , il y a deux formes ambiguës simples par genre et on trouve ici

Proposition A_4.- Si $p \equiv 5 \pmod 8$ ou $(\frac{p}{q}) = -1$, (C_2) est du type $C(2).C(2)$, l'équivalence des formes ambiguës simples et les facteurs principaux sont déterminés par les caractères génériques.

b) Supposons $p \equiv 1 \pmod 8$ et $(\frac{p}{q}) = 1$: Alors $r_4 = 1$, $V = p$ et la forme g est le genre principal. Si $q \equiv 3 \pmod 8$ $(\varepsilon'' = -1)$, $\bar{h}$ et $\bar{k}$ sont dans le genre principal ; si $q \equiv -1 \pmod 8$, h et k sont dans le genre principal.

On voit que pour toute racine carrée de g , on a (cf. lemme 3) :

$$e_V(\sqrt{g}) = (\frac{2q}{p})_4 .$$

b_1) Si $q \equiv 3 \pmod 8$, $2pq = 2B^2 + 4C^2$, donc toute forme $[B,2C,-2B]$ a pour carré h . Donc, on trouve ici :

Théorème B_4.- Soit $D = 2pq$, tel que $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ et $(\frac{q}{p}) = 1$. Alors $p = u^2 + 2v^2$, $q = w^2 + 2z^2$, $(\frac{uw+2vz}{p})$ ne dépend pas des signes de u , v , w , z et :

a) $(C_2) = C(\nearrow 8).C(2)$ si, et seulement si, $(\frac{uw+2vz}{p}) = (\frac{2q}{p})_4 = 1$.

b) Si $(\frac{uw+2vz}{p}) = -1$, $(\frac{2q}{p})_4 = 1$, f est équivalente à h et représente p et $-2q$.

c) Si $(\frac{uw+2vz}{p}) = 1$ et $(\frac{2q}{p})_4 = -1$, f est équivalente à $\bar{g}$ et représente -2 .

d) Si $(\frac{uw+2vz}{p}) = (\frac{2q}{p})_4 = -1$, f est équivalente à $\bar{k}$ et représente $-2p$ et q .

Cas particuliers : Si un genre de déterminant $-2q$ ne contient qu'une classe, c'est-à-dire pour $q = 3$ et 11, alors, si $(\frac{p}{q}) = 1$, $p = X^2 + 2qY^2$ et $[X,2qY,-2qX]^2 = g$. On voit alors que $(\frac{2q}{p})_4 = (\frac{X}{p})$ et, tenant compte, pour $q = 3$, de la formule du produit appliquée aux racines carrées de g et h ($(\frac{m}{p}) = (\frac{m}{3})(\frac{2}{m})(\frac{-1}{m})$), on trouve, pour $q = 3$ ($w = z = 1$) :

Corollaire B_4.- Soit $p = u^2 + 2v^2 = X^2 + 6Y^2 \equiv 1 \pmod{24}$ et soit $D = 6p$.

$(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $u + 2v$ et X sont congrus à ± 1 ou $\pm 5 \pmod{24}$.

Si $u + 2v \equiv \pm 1$ ou ± 5 et $X \equiv \pm 7$ ou $\pm 11 \pmod{24}$, f représente -2.

Si $u + 2v \equiv \pm 7$ ou ± 11 et $X \equiv \pm 1$ ou $\pm 5 \pmod{24}$, f représente -6.

Si $u + 2v \equiv \pm 7$ ou ± 11 et $X \equiv \pm 1$ ou $\pm 5 \pmod{24}$, f représente 3.

Il y a un résultat analogue pour $D = 22p$.

b_2) Si $q \equiv -1 \pmod 8$, $pq = G^2 - 2E^2 = 2E'^2 - G'^2$ et $2pq = 4E'^2 - 2G'^2$, donc $[G',2E',2G']^2 = g$. En outre, on voit que $G' = 2E + G$, $E' = E + G$, d'où, en fonction des décompositions de p et q : $G' = sd + 2(es+dr+er)$. On trouve donc ici

Théorème B_5.- Soit $D = 2pq$, où $p \equiv 1 \pmod 8$, $q \equiv -1 \pmod 8$ et $(\frac{p}{q}) = 1$. On a : $p = 2e^2 - d^2$ et $q = 2r^2 - s^2$. Soit $G' = sd + 2(es+dr+er)$. Le nombre $(\frac{G'}{p})$ ne dépend que de p et q et :

a) $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{G'}{p}) = (\frac{2p}{q})_4 = 1$. Sinon $(C_2) = C(4).C(2)$.

b) Si $(\frac{G'}{p}) = -1$, $(\frac{2q}{p})_4 = 1$, f est équivalente à h et représente p et $-2q$.

c) Si $(\frac{G'}{p}) = 1$ et $(\frac{2q}{p})_4 = -1$, f est équivalente à g et représente 2.

d) Si $(\frac{G'}{p}) = (\frac{2q}{p})_4 = -1$, f est équivalente à k et représente $2p$ et $-q$.

Si $q \equiv -1 \pmod 8$, il y a toujours au moins deux classes dans le genre principal de déterminant $-2q$, donc il n'y a pas ici de corollaires comme pour $q = 3$, 7 et $2q = 6$, 22.

Exemple numérique : $D = 646 = 2.17.19$, $p = 17$, $q = 19 \equiv 3 \pmod 8$, $17 = 3^2 + 2.2^2$, $19 = 1^2 + 2.3^2$, $(\frac{uw+2vz}{p}) = (\frac{19}{17}) = 1$, $(\frac{29}{p})_4 = (\frac{38}{17})_4 = (\frac{2}{17}) = 1$.

646 est le plus petit $D > 0$ tel que $(C_2) = C(\not\geqslant 8).C(2)$ (cf. [1]).

§ 7.- Etude de certains cas où $r_2 > 2$ et $r_4 = 1$.

A) Soit $D = qp_1 \dots p_n$, tel que $(\frac{q}{p_i}) = 1$, $(\frac{p_i}{p_j}) = -1$, $p_i \equiv 1 \pmod 8$ pour $i = 1, 2 \dots n$, où $n =$ 2 ou un nombre impair.

Les caractères génériques sont $(\frac{m}{q})$, $(\frac{m}{p_1})$, ... , $(\frac{m}{p_n})$, $(-1)^{\frac{m-1}{2}}$ et les formes ambiguës simples du genre principal sont, si $P = \prod p_i$ et $\varepsilon = (\frac{2}{q})$:

$$f = [1, 0, -D] \ , \ g = [P, 0, -q] \ , \ h = \left[2\varepsilon, \varepsilon, \frac{1-P}{2} q_i \varepsilon\right] \ , \ k = \left[2P\varepsilon, P\varepsilon, \frac{q-P}{2}\varepsilon\right] .$$

Une forme ambiguë simple est équivalente à g_1 ou h_1 où :

$$g_1 = \left[\pm P_1, 0, \mp q\ P_2\right] \ , \ h_1 = \left[\pm 2P_1, \pm P_1, \mp\frac{P_2 q - P_1}{2}\right] \ (P = P_1\ P_2) .$$

Calculons $e_{2q}(g_1)$ et $e_{2q}(h_1)$:

$$e_{2q}(g_1) = \pm\left(\frac{\pm P_1}{q}\right) = 1 \ ; \ e_q(h_1) = \left(\frac{\pm 2P_1}{q}\right) = \pm\varepsilon .$$

D'autre part, $\frac{P_2 q - P_1}{2} \equiv -1 \pmod 4$ si $q \equiv -1 \pmod 8$ et $\frac{P_2 q - P_1}{2} \equiv 1 \pmod 4$ si $q \equiv 3 \pmod 4$, donc $e_2(h_1) = \pm\varepsilon$, donc $e_{2q}(h_1) = 1$.

On a donc : $r_4 = 1$ et $V = 2q$.

A_1) Si $q \equiv 3 \pmod 8$. Soit $p_i = u_i^2 + 2v_i^2$, $P = U^2 + 2V^2$, $q = w^2 + 2z^2$.

On voit que le premier coefficient d'une racine carrée de h est $Uz + Vw$.

Posons $\alpha = (\frac{Uz+Vw}{P})$. D'une part : $\alpha = (\frac{Uz+Vw}{q})(\frac{1}{Uz+Vw})$.

D'autre part : $(\frac{Uz+Vw}{p_i}) = (\frac{V}{p_i})(\frac{z+\lambda w}{p_i})$ et $(\frac{u_i z+v_i w}{p_i}) = (\frac{v_i}{p_i})(\frac{z+\lambda' w}{p_i})$ où λ et λ' sont racines carrées de -2 modulo p_i .

Comme $(\frac{V}{p_i}) = (\frac{p_i}{V'}) = 1$ et $(\frac{v_i}{p_i}) = (\frac{p_i}{v_i'}) = 1$ (le $'$ désigne la partie impaire) et comme $(z+\lambda w)(z-\lambda w) \equiv q \pmod{p_i}$ et puisque $(\frac{q}{p_i}) = 1$, on trouve :

$$\alpha = \prod_i (\frac{u_i z+v_i w}{p_i}) .$$

A_2) Si $q \equiv -1 \pmod 8$. Soit $p_i = 2e_i^2 - d_i^2$, $P = 2E^2 - D^2$, $q = 2r^2 - s^2$.

Ici le premier coefficient d'une racine carrée de h est $Es + Dr$.

Posons $\alpha = (\frac{Es+Dr}{P})$. D'une part : $(\frac{Es+Dr}{P}) = (\frac{Es+Dr}{P})(\frac{1}{Es+Dr})$.

D'autre part, comme ci-dessus, on voit que : $(D^2 E^{-2} \equiv 2 \pmod{p_i}) \dots$

$$\alpha = \prod_i (\frac{e_i s+d_i r}{p_i}) .$$

Utilisant le lemme 3, on obtient, avec les notations et hypothèses ci-dessus :

Proposition B_5.- Soit $D = qp_1 \dots p_n = qp$, tel que $(\frac{q}{p_i}) = 1$, $(\frac{p_i}{p_j}) = -1$, $p_i \equiv 1 \pmod 8$ $(1 \leq i < j \leq n)$ et où $n = 2$ ou un nombre impair.

Alors $(C_2) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $\alpha = (\frac{q}{P})_4 = 1$. Sinon $(C_2) = C(4).C(2)^{n-1}$.

Si $\alpha = 1$, $(\frac{q}{P})_4 = -1$, f est équivalente à h et représente $2\varepsilon"$ $(\varepsilon" = (\frac{2}{q}))$.

Si $\alpha = -1$, $(\frac{q}{P})_4 = 1$, f est équivalente à g et représente $-q$.

Si $\alpha = (\frac{q}{P})_4 = -1$, f est équivalente à k et représente $-2q\varepsilon"$.

B) Soit $D = 2q\ p_1 \ldots p_n$, où n est impair, $(\frac{q}{p_i}) = 1$, $p_i \equiv 1 \pmod 8$, $(\frac{p_i}{p_j}) = -1$. Les caractères génériques sont $(\frac{m}{p_i})$, $(\frac{m}{q})^i$, $(\frac{-2}{m})$.

Les formes ambiguës simples du genre principal sont : si $P = p_1 \ldots p_n$ et $\varepsilon" = (\frac{2}{q})$:

$$f = [1,0,-D] \ , \ g = [P,0,-2q] \ , \ h = [2\varepsilon",0,-\varepsilon"Pq] \ , \ k = [2\varepsilon"P,0,-\varepsilon"q] \ .$$

On vérifie que les classes ambiguës donnent aux caractères toutes les combinaisons de valeurs telles que $e_{2q} = 1$, d'où, en posant, suivant que $\varepsilon" = -1$ ou $\varepsilon" = 1$ et raisonnant comme en A :

$$\beta = (\frac{Uw+2Vz}{P}) = \prod_i (\frac{u_i w+2v_i z}{p_i}) = (\frac{Uw+2Vz}{q})\ (\frac{1}{Uw+2Vz})$$

$$= (\frac{(s+2r)D+2(s+r)E}{P}) = \prod_i (\frac{(s+2r)d_i+2(s+r)e_i}{p_i}) = (\frac{(s+2r)D+2(s+r)E}{q})\ (\frac{-1}{(s+2r)D+2(s+r)E}) \ .$$

Proposition B_6.- Soit $D = 2q\ p_1 \ldots p_n = 2qP$, où n est impair, $(\frac{q}{p_i}) = 1$, $p_i \equiv 1 \pmod 8$ et $(\frac{p_i}{p_j}) = -1$ $(1 \leqslant i < j \leqslant n)$.

Alors $(C_2) = C(\geqslant 8).C(2)^n$ si, et seulement si, $\beta = (\frac{2q}{P}) = 1$.

Si $\beta = 1$ et $(\frac{2q}{P})_4 = -1$, f représente $2\varepsilon"$ $(f \approx h)$.

Si $\beta = -1$ et $(\frac{2q}{P})_4 = 1$, f représente $-2q$ $(f \approx g)$.

Si $\beta = (\frac{2q}{P})_4 = -1$, f représente $-\varepsilon"q$ $(f \approx k)$.

§ 8 - Racine carrée de la forme $g = [M,0,N]$ quand elle est dans le genre principal de déterminant D et quand M est impair si $N \equiv 1 \pmod 4$.

D'après Gauss (DA, § 286, cf. aussi [13], ch. VII, p. 161 et [18]), on obtient une racine carrée de $g = [M,0,N]$ par la méthode suivante :

Soient α , α' , α'' , β , β' , β'' une solution quelconque de :

(1) $M = \alpha^2 - 2\alpha'\alpha''$, (2) $\beta = \alpha'\beta'' + \alpha''\beta'$, (3) $N = \beta^2 - 2\beta'\beta''$.

Posons : $A = \alpha\beta' - \alpha'\beta$, $B = \alpha''\beta' - \alpha'\beta''$, $C = \alpha''\beta - \alpha\beta''$.

Alors un au moins des nombres A , C est impair ; quand A est impair, $\psi = [A,B,2C]$ est une racine carrée de g et $\psi' = [2A,B,C]$ quand C est impair.

Le lemme 5 montre que N est représenté par une forme φ du genre principal de déterminant N . Soit k , choisi premier à 2D , le premier coefficient d'une racine carrée de φ ; il existe des entiers X , Y , ℓ et m' tels que :

(4') $M = k^2 X^2 + 2\ell XY + m' Y^2$; $N = \ell^2 - k^2 m'$.

On peut modifier ℓ modulo k^2 , donc choisir $\ell \equiv N \pmod 2$. Alors $m' = 2m$, où m est pair si $N \equiv 1 \pmod 4$, impair sinon. Les relations (4') s'écrivent :

(4) $M = k^2 X^2 + 2Y(\ell X+mY)$; $N = \ell^2 - 2k^2 m$.

Les valeurs de M et N conduisent à poser :

$$\alpha = kX \ , \ \beta = \ell \ , \ \alpha' = -Y \ , \ \alpha'' = \ell X + mY \ .$$

(1), (2) et (3) sont alors vérifiées si l'on pose $\beta' = k$, $\beta'' = km$. C'est clair pour (1) et (3) et avec les valeurs ci-dessus (2) s'écrit :

$$k\ell X = -Ykm + (\ell X+mY)\,k \ .$$

On trouve :

$$A = k^2 X + \ell Y \ ; \ B = k(\ell X+2mY) \ ; \ C = NX + mA \ .$$

Etudions la parité de A . On sait que X a la parité de M et ℓ celle de N

a) Si M est pair et $N \equiv -1 \pmod 4$, Y est impair (car $M \equiv 2 \pmod 4$) , donc A est impair.

b) Si N est pair et M impair, A est impair.

c) Si $M \equiv N \equiv 1 \pmod 4$, Y est pair, donc A est impair.

d) Si $M \equiv -1$, $N \equiv 1 \pmod 4$, Y est impair, donc A est pair.

e) Si $M \equiv 1$, $N \equiv -1 \pmod 4$, m est impair, donc $Y(\ell X+mY)$ est toujours pair, donc ici, on ne peut pas déterminer à priori la parité de A .

(Le cas $M \equiv N \equiv -1 \pmod 4$ est impossible, car on aurait : $e_2(g) = -1$)

Le nombre $A = k^2 X + \ell Y$ est premier à D. En effet, l'équation (4) entraîne :

$$k^2 M = (k^2X+\ell Y)^2 - NY^2 = A^2 - NY^2 .$$

Comme k est premier à D, on voit qu'un diviseur premier commun à A et D diviserait à la fois M et N.

Nous avons donc démontré le résultat suivant :

Lemme 8.- Soit $[M,0,N]$ une forme du genre principal de déterminant D telle que M soit impair si $N \equiv 1 \pmod 4$. Il existe des entiers relatifs k, ℓ, m, X, Y tels que k soit premier à $2D$ et que :

(4) $$m = k^2X + 2\ell XY + 2m\,Y^2 \quad ; \quad N = \ell^2 - 2k^2 m .$$

Soit A le nombre $k^2 X + \ell Y$. Alors :

a) Le nombre A est premier à D et impair si $D \equiv 1 \pmod 4$, pair si $D \equiv -M \equiv N \equiv 1 \pmod 4$.

b) Si le nombre A est impair, il est le premier coefficient d'une des racines carrées ψ de $[M,0,N]$; s'il est impair, le nombre $2A$ est le premier coefficient d'une des racines carrées ψ' de $[M,0,N]$.

c) Ce premier coefficient A ou $2A$ est toujours premier au nombre D et détermine les valeurs de tous les caractères génériques de ψ ou de ψ'.

Corollaire (Complément au lemme 6).- Si $M = x^2 - Ny^2$ avec x pair, une des racines carrées de $[M,0,N]$ a pour premier coefficient $2x$.

Si l'on pose $x = X + Y$, $y = Y$, on trouve en effet :

$$M = (X+Y)^2 - NY^2 = X^2 + 2XY + (1-N)\,Y^2$$

C'est l'équation (4) avec $k = \ell = 1$, donc $A = X + Y = x$ C. Q. F. D.

On peut démontrer ce corollaire par un calcul direct (cf. [13], p. 123). Par l'une ou l'autre méthode, la racine carrée de $[M,0,N]$ que l'on trouve est :

$$\psi' = \left[2x, x-Ny, x\tfrac{1-N}{2}+Ny\right] .$$

Exemple d'application du lemme 8 (cf. théorème B_2) : Soit $D = 11p$ où $p \equiv 1 \pmod 8$ et $\left(\frac{p}{11}\right) = 1$. Alors $p = u^2 + 2v^2$: $11 = 3^2 + 2.1^2$. Donc, dans le théorème B_2, $w = 3$, $z = 1$. La forme g est $[p,0,-11]$; posons $M = p$, $N = -11$; les classes (au sens large) de déterminant 11 sont dans le genre principal et leurs représentants sont $F = [1,0,11]$ et $G = [3,1,4]$.

Il est clair que G représente 9 (pour $x = y = 1$), donc par la transformation $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$, G devient $G' = 9X^2 + 10XY + 4Y^2$. Pour G', $k = 3$, $\ell = 5$ et si (x,y) est une représentation de p par G', on a : $k^2 X + \ell Y = 9X + 5Y = 4x + 5y$ où (x,y) est une représentation de p par G. Posons $\zeta = x$ si $p = x^2 + 11y^2$, ou bien $\zeta = 4x + 5y$ si $p = 3x^2 + 2xy + 4y^2$, nous obtenons avec

les notations ci-dessus :

Proposition B_7.- Soit $D = 11p$ où $p \equiv 1 \pmod 8$ et $\left(\frac{p}{11}\right) = 1$. Posons $e_{22}(m) = \left(\frac{m}{11}\right)\left(\frac{-1}{m}\right)$. Alors : $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $e_{22}(3u+v) = e_{22}(\zeta) = 1$. Sinon $(C_2) = C(4).C(2)$.

Si $e_{22}(3u+v) = e_{22}(\zeta) = -1$, alors 22 est facteur principal.

Si $e_{22}(3u+v) = 1$, $e_{22}(\zeta) = -1$, alors -11 est facteur principal.

Si $e_{22}(3u+v) = -1$, $e_{22}(\zeta) = 1$, alors -2 est facteur principal.

§ 9.- Cas de $D = pqq'$, où $p \equiv -q \equiv -q' \equiv 1 \pmod 4$ et $\left(\frac{q}{q'}\right) = 1$, $\left(\frac{q'}{q}\right) = -1$.

Posons $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \varepsilon$ et $\left(\frac{p}{q'}\right) = \left(\frac{p'}{q}\right) = \varepsilon'$. Les formes ambiguës simples sont :

$$f = [1,0,-pqq'] \ , \ g = [p,0,-qq'] \ , \ h = [q,0,-pq'] \ , \ h' = [q',0,-pq]$$
$$\bar{f} = [-1,0,pqq'] \ , \ \bar{g} = [-p,0,qq'] \ , \ \bar{h} = [-q,0,pq'] \ , \ \bar{h}' = [-q',0,pq] \ .$$

La valeur des caractères pour ces formes est :

	f	$\bar{f}$	g	$\bar{g}$	h	$\bar{h}$	h'	$\bar{h}'$
$\left(\frac{m}{p}\right)$	1	1	$\varepsilon\varepsilon'$	$\varepsilon\varepsilon'$	ε	ε	ε'	ε'
$\left(\frac{m}{q'}\right)$	1	-1	ε	$-\varepsilon$	ε	$-\varepsilon$	-1	1
$\left(\frac{m}{q}\right)$	1	-1	ε'	$-\varepsilon'$	1	-1	$-\varepsilon'$	ε'

Proposition A_5.- Si $-\varepsilon$ ou $\varepsilon' = -1$, deux de ces formes sont dans le genre principal. $(C_2) = C(2)^2$ et les facteurs principaux sont déterminés par les caractères génériques.

Supposons donc $\varepsilon = \varepsilon' = 1$. Le genre principal contient f , g , h , $\bar{h}'$, donc $r_4 = 1$; les caractères des classes ambiguës sont 1 , 1 , 1 et 1 , -1 , -1 , donc $V = p$.

Appliquons le lemme 1 à la forme $g = [p,0,-qq']$ et le lemme 8 à la forme $\bar{h}' = [-q',0,pq]$ en prenant $M = pq$ et $N = -q'$, on obtient par la méthode B :

Théorème B_6.- Soit $D = pqq'$ où $p \equiv -q \equiv -q' \equiv 1 \pmod 4$ et $\left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right) = \left(\frac{q'}{q}\right) = 1$. Il existe des entiers X , Y , k , ℓ , m , tels que :

$$pq = k^2 X^2 + 2\ell XY + 2m Y^2 \ ; \ -q' = \ell^2 - 2k^2 m \ .$$

Posons $\alpha = \left(\frac{qq'}{p}\right)_4$ et $\beta = \left(\frac{2(k^2X+Y)}{p}\right)$. Le nombre β ne dépend que de p , q , q' et $(C_2) = C(\geqslant 4).C(2)$.

Pour que $(C_2) = C(\geqslant 8).C(2)$, il faut et il suffit que $\alpha = \beta = 1$.

Si $\alpha = 1$ et $\beta = -1$, $-qq'$ est facteur principal $(f \approx g)$.
Si $\alpha = -1$ et $\beta = 1$, $-q'$ est facteur principal $(f \approx \bar{h}')$.
Si $\alpha = \beta = -1$, q est facteur principal $(f \approx h)$.

Au lieu du caractère β , on aurait pu prendre d'autres caractères en posant $M = -q'$, $N = pq$ pour $\bar{h}'$, ou bien en utilisant la forme $h = [q,0,-pq']$. On obtient des résultats analogues au théorème B_6, mais un peu moins simples.

Cas particuliers :

1) Cas où il y a une seule classe de déterminant $-q'$. ($q' = 3$ et 7) .

Si $r_4 = 1$, c'est-à-dire si $\left(\frac{p}{q'}\right) = \left(\frac{p}{q}\right) = 1$, alors $pq = x_1^2 + q'y^2$ où nécessairement, x_1 est pair et y impair. Posons : $X + Y = x_1$ et $Y = y$; on a : $pq = X^2 + 2XY + (1+q')Y^2$ et $k^2 X + Y = X + Y = x_1$, donc $\beta = \left(\frac{2x_1}{p}\right)$ et on trouve :

Proposition B_8.- Soit $D = pqq'$ où $q' = 3$ ou 7 et $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = \left(\frac{q'}{q}\right) = 1$. Alors $pq = 4x^2 + q'y^2$ et :

$(C_2) = C(\not\equiv 8).C(2)$ si, et seulement si, $\left(\frac{q'q}{p}\right)_4 = \left(\frac{x}{p}\right) = 1$.

Si $\left(\frac{q'q}{p}\right)_4 = \left(\frac{x}{p}\right) = -1$, f représente q et $-q'p$.

Si $\left(\frac{q'q}{p}\right)_4 = 1$ et $\left(\frac{x}{p}\right) = -1$, f représente p et $-q'q$.

Si $\left(\frac{q'q}{p}\right)_4 = -1$ et $\left(\frac{x}{p}\right) = 1$, f représente $-q'$ et pq.

Etudions en particulier le cas où $D = 21p$ $(q' = 3, q = 7)$.

On a $(C_2) = C(\not\equiv 4).C(2)$ si, et seulement si, $p \equiv 1 \pmod{12}$ et $\left(\frac{p}{7}\right) = 1$, c'est-à-dire si $p \equiv 1$, 25 ou $37 \pmod{84}$. Alors :

$$p = X^2 + 3Y^2 = X'^2 + 7Y'^2 \quad ; \quad 7 = 2^2 + 3.1^2 \quad ; \quad 7p = (2X+3Y)^2 + 3(X-2Y)^2 .$$

Ici $\alpha = \left(\frac{21}{p}\right)_4 = \left(\frac{X}{p}\right)\left(\frac{X'}{p}\right)$ et $\beta = \left(\frac{2(2X+3Y)}{p}\right) = \left(\frac{2X+3Y}{7}\right)\left(\frac{X}{3}\right)$.

Choisissons les signes de X et X' de manière qu'ils soient congrus à 1 modulo 4. La formule du produit appliquée à $[X,Y,-3X]$ et $[X',Y',-7X']$ montre que $\alpha = \left(\frac{X}{3}\right)\left(\frac{X'}{7}\right)$. Donc, avec les hypothèses et notations ci-dessus, on a :

Corollaire B_8.- Soit $D = 21p$ tel que $p \equiv 1 \pmod{12}$ et $\left(\frac{p}{7}\right) = 1$. Alors $p = X^2 + 3Y^2 = X'^2 + 7Y'^2$. Si $X \equiv X' \equiv 1 \pmod 4$, on a :
$(C_2) = C(\not\equiv 8).C(2)$ si, et seulement si, $\left(\frac{X}{3}\right) = \left(\frac{X'}{7}\right) = \left(\frac{2X+3Y}{7}\right)$.
Sinon $(C_2) = C(4).C(2)$ et :

Si $\left(\frac{X}{3}\right) = -\left(\frac{X'}{7}\right) = -\left(\frac{2X+3Y}{7}\right)$, $t^2 - 21pu^2$ représente $+7$.

Si $\left(\frac{X}{3}\right) = \left(\frac{X'}{7}\right) = -\left(\frac{2X+3Y}{7}\right)$, $t^2 - 21pu^2$ représente -21.

Si $\left(\frac{X}{3}\right) = -\left(\frac{X'}{7}\right) = \left(\frac{2X+3Y}{7}\right)$, $t^2 - 21pu^2$ représente -3.

2) Cas où il y a une seule classe par genre de déterminant q, pq ou p.

On peut alors appliquer le lemme 7 aux formes h, $\bar{h}'$ ou g respectivement. Par exemple, si ces trois conditions sont simultanément réalisées, on obtient, en utilisant les notations du théorème B_6 :

Proposition B_9.- Soit $D = pqq'$ tel que $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = \left(\frac{q}{q'}\right) = 1$ et qu'il y ait une seule classe par genre de déterminant p, q et pq. Alors $p \equiv 5 \pmod 8$ et il existe des nombres x, y, x', y', x'', y'' tels que :

$$-qq' = x^2 - py^2 \quad ; \quad -pq' = x'^2 - qy'^2 \quad ; \quad -q' = x''^2 - pqy''^2 .$$

Les nombres $\left(\frac{x}{p}\right)$, $\left(\frac{x'}{p}\right)$ et $\left(\frac{x''}{p}\right)$ ne dépendent que de D et vérifient :

$$\left(\frac{x}{p}\right) = \left(\frac{qq'}{p}\right)_4 = \quad ; \quad \left(\frac{x''}{p}\right) = \beta \quad ; \quad \left(\frac{x}{p}\right)\left(\frac{x'}{p}\right)\left(\frac{x''}{p}\right) = 1 .$$

Pour que $(C_2) = C(\not\equiv 8).C(2)$, il faut et il suffit que $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right) = \left(\frac{x''}{p}\right) = 1$.

Sinon $(C_2) = C(4).C(2)$ et g, h ou $\bar{h}'$ est équivalente à f suivant que $\left(\frac{x}{p}\right) = 1$, $\left(\frac{x'}{p}\right) = 1$ ou $\left(\frac{x''}{p}\right) = 1$.

Généralisations et remarques : Soit $D = Pqq'$ où $P = p_1 \dots p_n$, $n = 1$, 2 ou impair, $(\frac{p_i}{p_j}) = -1$, $(\frac{p_i}{q}) = 1$, $(\frac{q}{q'}) = (\frac{q'}{q}) = 1$

Les caractères génériques sont $(\frac{m}{p_i})$, $(\frac{m}{q})$, $(\frac{m}{q'})$ et on voit que les formes ambiguës simples du genre principal sont équivalentes à :

$$f = [1,0,-D] \text{ , } g = [P,0,-qq'] \text{ , } h = [q,0,-Pq'] \text{ , } \bar{h}' = [Pq,0,-q'] \text{ .}$$

Une forme ambiguë simple est du type $g_1 = [\pm P_1,0,\mp P_2 qq']$ ou du type $k_1 = [-P_1 q,0,\mp P_2 q']$, avec $P_1 P_2 = P$. Calculons $e_{qq'}(g_1)$ et $e_{qq'}(h_1)$

$$e_{qq'}(g_1) = (\frac{\pm P_1}{q})(\frac{\pm P_1}{q'}) = 1 \text{ ; } e_{qq'}(h_1) = (\frac{-P_1 q}{q'})(\frac{\mp P_2 q'}{q}) = (\frac{\pm q}{q'})(\frac{\mp q'}{q}) = 1 \text{ .}$$

Considérons maintenant les racines carrées de $\bar{h}'$ et de g . On trouve un résultat semblable au théorème B_6, où p est remplacé par P et où $r_2 = n + 1$

Calcul de β : Soit ζ et ζ' les ordres impairs des classes de déterminant q' représentant P et q respectivement :

$P^{\zeta} = U^2 + q' V^2$ $q^{\zeta'} = U'^2 + q' V'^2$. Donc $Pq\sigma^2 = B^2 + q' C^2$ où $\sigma = P^{\eta} q^{\eta'}$ $(\zeta = 2\eta + 1$, $\zeta' = 2\eta' + 1)$. $B = UU' + q' VV'$ est pair.

$q' Pq\sigma^2 = B^2 q' + (q'C)^2$ montre que $[B,qC,-Bq']$ est une forme de déterminant $D\sigma^2$, improprement primitive. Le corollaire du lemme 8 montre qu'il existe une forme proprement primitive $\varphi = [2B,\dots,\dots]$, de déterminant $D\sigma^2$, de carré représentant $-q'$, donc équivalente à $[-q',0,Pq\sigma^2]$.

Comme $(\sigma,2B) = 1$, $\varphi \approx [2B,C',E']$ avec $C' \equiv 0 \pmod{\sigma}$;
$D^2 = C'^2\sigma^2 - BE'$ montre que $E' = E''\sigma^2$, donc $\varphi \approx [2B,C''\sigma,E''\sigma^2]$.

Or, on sait qu'il existe un homomorphisme du groupe des classes de déterminant $D\sigma^2$ proprement primitives sur celui des classes de déterminant D , où $[2B,C''\sigma,E''\sigma]^2$ devient $[2B,C'',E'']$ et $[-q',0,Pq\sigma^2]$ devient $[-q',0,Pq]$ (cf. [13], chapitre 6, § 7).

Une racine carrée de $[-q',0,Pq]$ a donc pour premier coefficient $2B$, ce qui prouve que :

$$\beta = (\frac{2B}{P}) = (\frac{2B}{qq'}) \text{ .}$$

§ 10 - Cas de $D = 2qq'$ où $(\frac{q}{q'}) = -(\frac{q'}{q}) = 1$.

On pose $(\frac{2}{q}) = \varepsilon$ et $(\frac{2}{q'}) = \varepsilon'$.

Les caractères génériques sont : $(\frac{m}{q})$, $(\frac{m}{q'})$, $(\frac{2}{m})$.

Les formes ambiguës simples sont équivalentes à :

$$f = [1,0,-2qq'] \ , \ g = [2,0,-qq'] \ , \ h = [q,0,-2q'] \ , \ h' = [q',0,-2q]$$
$$\bar{f} = [-1,0,2qq'] \ , \ \bar{g} = [-2,0,qq'] \ , \ \bar{h} = [-q,0,2q'] \ , \ \bar{h}' = [-q',0,2q] \ .$$

Le tableau des caractères pour ces formes est :

	f	$\bar{f}$	g	$\bar{g}$	h	$\bar{h}$	h'	$\bar{h}'$
$(\frac{m}{q})$	1	-1	ε	$-\varepsilon$	ε	$-\varepsilon$	-1	1
$(\frac{m}{q'})$	1	-1	ε'	$-\varepsilon'$	1	-1	$-\varepsilon'$	ε'
$(\frac{2}{m})$	1	1	$\varepsilon\varepsilon'$	$\varepsilon\varepsilon'$	ε	ε	ε'	ε'

Proposition A.- Si q ou q' est congru à 3 modulo 8 , $(C_2) = C(2)^2$ et les facteurs principaux sont déterminés par les caractères génériques.

Supposons donc $q \equiv q' \equiv -1 \pmod 8$. Les caractères des classes ambiguës sont 1 , 1 , 1 et -1 , -1 , 1 , donc $V = 2$ et les formes ambiguës simples du genre principal sont f , g , h et $\bar{h}'$, donc $r_4 = 1$.

Le lemme 2 montre que une des racines carrées de g est dans le genre principal si, et seulement si, $qq' \equiv 1 \pmod{16}$.

Considérons $h = [q,0,-2q']$ et posons $M = q$, $N = -2q'$. Comme le nombre $k^2 X + \ell Y$ du lemme 8 est impair et congru à $X + \ell Y$ modulo 8 , on obtient :

Théorème B.- Soit $D = 2qq'$ où $q \equiv q' \equiv -1 \pmod 8$ et $(\frac{q}{q'}) = 1$. Il existe des entiers X , Y , k , ℓ , m tels que k soit premier à D et que :

$$q = k^2 X^2 + 2\ell XY + 2m Y^2 \ ; \ -2q' = \ell^2 - 2k^2 m \ .$$

Le nombre $\beta = (\frac{2}{X+\ell Y})$ ne dépend que de q et q' et :

a) $(C_2) = C(\geq 8).C(2)$ si, et seulement si, $\beta = 1$ et $q \equiv q' \pmod{16}$. Sinon $(C_2) = C(4).C(2)$.

b) Si $\beta = 1$ et $q \equiv q' + 8 \pmod{16}$, q est facteur principal ($f \approx h$) .

c) Si $\beta = -1$ et $q \equiv q' \pmod{16}$, 2 est facteur principal ($f \approx g$) .

d) Si $\beta = -1$ et $q \equiv q' + 8 \pmod{16}$, $2q$ est facteur principal ($f \approx \bar{h}'$) .

Cas particulier : $q' = 7$ $D = 14q$ où $q \equiv -1 \pmod 8$ et $(\frac{q}{7}) = +1$.

Il y a deux classes : $[1,0,14]$ et $[7,0,2]$ dans le genre principal de discriminant -14 . Deux cas sont possibles :

$q = X^2 + 14Y^2$. Alors $k = 1$, $\ell = 0$ et $\beta = (\frac{2}{X})$

$q = 7X^2 + 2Y^2 = 9x^2 + 4xy + 2y^2$ où $X = x$, $Y = x + y$.

Ici, $x + \ell y = x + 2y = Y + y = 2Y - X$, donc $\beta = \left(\frac{2}{2Y-X}\right) = \left(\frac{2}{X+2Y}\right)$.

Posons donc $\zeta = X$ si $q = X^2 + 14Y^2$, $\zeta = X + 2Y$ si $q = 7X^2 + 2Y^2$:

Proposition B_{10}.- Soit $D = 14q$ où $q \equiv -1 \pmod 8$ et $\left(\frac{q}{7}\right) = 1$ ($q \equiv 15$, 23 ou 39 (mod 56)) .

$(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $\zeta = \pm 1 \pmod 8$ et $q \equiv 7 \pmod{16}$.

Si $\zeta^2 \equiv 1$ et $q \equiv -1 \pmod{16}$, -7 est facteur principal.

Si $\zeta^2 \equiv 9$ et $q \equiv 7 \pmod{16}$, 2 est facteur principal.

Si $\zeta^2 \equiv 9$ et $q \equiv -1 \pmod{16}$, -14 est facteur principal.

Exemple numérique : $D = 994 = 2.7.71 = 14q$, $q = 71$.

$(C_2) = C(\geqslant 8).C(2)$. On a bien : $71 \equiv 7 \pmod{16}$ et en outre : $71 = 7.3^2 + 2.2^2$, donc ici : $X + 2Y = 3 + 4 = 7 \equiv -1 \pmod 8$.

Au lieu d'utiliser la forme h avec $M = q$, $N = -2q'$, on aurait pu poser $M = -2q'$, $N = q$, ou bien utiliser la forme $\bar{h}'$ avec $M = -q'$, $N = 2q$. Ceci est particulièrement intéressant dans les cas, très fréquents, où il y a une seule classe par genre de déterminant q , ou bien $2q$, car on peut alors utiliser le lemme 6. Ainsi :

Proposition B_{11}.- Soit $D = 2qq'$ où $q \equiv q' \equiv -1 \pmod 8$, $\left(\frac{q}{q'}\right) = 1$ et où il y a une seule classe dans chaque genre de déterminant q et $2q$. On a :

$$-2q' = x^2 - qy^2 \quad ; \quad -q' = x'^2 - 2qy'^2 .$$

Posons $\alpha = (-1)^{\frac{q'-q}{8}}$, $\beta = \left(\frac{2}{x}\right)$, $\beta' = \left(\frac{2}{x'}\right)$. Alors :

a) Les nombres β et β' ne dépendent que de q et q' et $\alpha\beta\beta' = 1$.

b) Pour que $(C_2) = C(\geqslant 8).C(2)$, il faut et il suffit que $\alpha = \beta = \beta' = 1$. Sinon $(C_2) = C(4).C(2)$ et 2 , q ou $2q$ est facteur principal suivant que $\alpha = 1$, $\beta = 1$ ou $\beta' = 1$.

Les nombres premiers $q \equiv -1 \pmod 8$ tels qu'il y ait une seule classe par genre de déterminants q et $2q$ sont très nombreux (10 sur 12 jusqu'à 200 par exemple).

Exemple numérique : $D = 4534 = 2.7.311$; $q = 7$, $q' = 311$; $q' - q = 304 = 16.19$. On a : $-622 = 15^2 - 7.11^2$; $-311 = 33^2 - 14.10^2$: $x = 15$, $x' = 33$.

Donc $\alpha = \beta = \beta' = 1$ et $(C_2)\ (4534) = C(\geqslant 8).C(2)$.

4534 est le plus petit $D > 0$ tel que $(C_2^*) = C(\geqslant 16).C(2)$.

§ 11.- Cas des corps imaginaires $(D < 0)$.

La méthode précédente s'applique aux cas où $D < 0$. Le problème est plus simple, car il y a une seule forme ambiguë simple par classe ambiguë.

Les cas où (C_2) est cyclique sont connus (cf. par exemple [11]). Nous allons étudier dans ce paragraphe les cas où (C_2) est produit de deux groupes cycliques :

$$D = -pp' , -2pp' , -qpp' , 2pq , -qq'q" , -qq' , -2pq , -2qq' .$$

Cas 1) : $D = -pp'$. Les caractères génériques sont $(\frac{m}{p})$, $(\frac{m}{p'})$, $(\frac{-1}{m})$. Les formes ambiguës simples sont équivalentes à :

$$f = [1,0,pp'] , g = [p,0,p'] , h = \left[2,1,\frac{1+pp'}{2}\right] , k = \left[2p,p,\frac{p+p'}{2}\right] .$$

Tableau des caractères : On pose $(\frac{p}{p'}) = \varepsilon$; $(\frac{2}{p}) = \varepsilon'$; $(\frac{2}{p'}) = \varepsilon"$

	f	g	h	k
$(\frac{m}{p})$	1	ε	ε'	$\varepsilon\varepsilon'$
$(\frac{m}{p'})$	1	ε	$\varepsilon"$	$\varepsilon\varepsilon"$
$(\frac{-1}{m})$	1	1	$\varepsilon'\varepsilon"$	$\varepsilon'\varepsilon"$

a) Si $\varepsilon = \varepsilon' = -1$, $\varepsilon" = 1$, ou bien si $\varepsilon = \varepsilon" = -1$, $\varepsilon' = 1$, il n'y a pas de forme ambiguë simple autre que f dans le genre principal, donc $(C_2) = C(2)^2$.

b) Si $\varepsilon = \varepsilon' = \varepsilon" = -1$, c'est-à-dire si $p \equiv p' \equiv 5 \pmod 8$ et $(\frac{p}{p'}) = -1$.

Alors k est dans le genre principal, donc $(C_2) = C(\nearrow 4).C(2)$.

Soit m , choisi premier à 2pp' le premier coefficient d'une racine carrée de k :

(1) $m^2 = 2px^2 + 2pxy + \frac{p+p'}{2} y^2$ avec y impair et premier à p , d'où :

(2) $2m^2 = p(2x+y)^2 + p' y^2$; (3) $(2m)^2 = 2p(2x+y)^2 + 2p' y^2$.

Comme $2m^2 \equiv 2 \pmod{16}$ et $p' \equiv p' y^2 \equiv 5 \pmod 8$, on déduit de (2) :

$p(2x+y)^2 - 1 \equiv 1 - p' y^2 \equiv p' y^2 - 1 + 8 \pmod{16}$, d'où :

(4) $$(\frac{2}{2x+y}) (\frac{2}{y}) = -(-1)^{\frac{p-p'}{8}} = (\frac{pp'}{2})_4 ,$$

la dernière égalité étant vraie parce que $p \equiv p' \equiv 5 \pmod 8$.

D'autre part, l'équation (3) montre que :

$$(\frac{2m}{p}) = (\frac{2p'}{p})_4 (\frac{y}{p}) = (\frac{2p'}{p})_4 (\frac{p}{y}) = (\frac{2p'}{p})_4 (\frac{2}{y}) \quad \text{et} \quad (\frac{2m}{p'}) = (\frac{2p}{p'})_4 (\frac{2}{2x+y}) .$$

Comme $(\frac{2}{p}) = (\frac{2}{p'}) = -1$, on voit que :

$$(\frac{-1}{m}) = (\frac{m}{p}) (\frac{m}{p'}) = (\frac{2m}{p}) (\frac{2m}{p'}) = (\frac{2p'}{p})_4 (\frac{2p}{p'})_4 (\frac{pp'}{2})_4 .$$

Les caractères des classes ambiguës sont 1 , 1 , 1 et -1 , -1 , 1 , donc $V = 2$:

Proposition B_1'.- Soit $D = -pp'$ où $p \equiv p' \equiv 5 \pmod 8$ et $\left(\frac{p}{p'}\right) = -1$.

$(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $\left(\frac{pp'}{2}\right)_4 \left(\frac{2p}{p'}\right)_4 \left(\frac{2p'}{p}\right)_4 = 1$.
Sinon $(C_2) = C(4).C(2)$.

Exemples :

1) $D = -65$; $(C_2) = C(4).C(2)$

$\left(\frac{pp'}{2}\right)_4 = 1$; $\left(\frac{10}{13}\right)_4 = \left(\frac{36}{13}\right)_4 = \left(\frac{6}{13}\right) = -\left(\frac{3}{13}\right) = -1$; $\left(\frac{26}{5}\right)_4 = 1$.

2) $D = -185 = -5.37$; $(C_2) = C(8).C(2)$

$\left(\frac{pp'}{2}\right)_4 = -1$; $\left(\frac{74}{5}\right)_4 = -1$; $\left(\frac{10}{37}\right)_4 = \left(\frac{84}{37}\right)_4 = \left(\frac{2}{37}\right)\left(\frac{21}{37}\right)_4 = -\left(\frac{-16}{37}\right)_4 =$
$= -\left(\frac{-1}{37}\right)_4 = 1$.

c) Cas où $\varepsilon = -1$, $\varepsilon' = \varepsilon'' = 1$: $\left(\frac{p}{p'}\right) = -1$, $p \equiv p' \equiv 1 \pmod 8$.

La forme h est dans le genre principal et si $pp' = 2e^2 - d^2$ $(e > 0)$, $[e,d,2e]^2 = h$. Les caractères des classes ambiguës sont 1 , 1 , 1 et -1 , -1 , 1 , donc $V = 2$ et, comme $\lambda(pp') = \left(\frac{-1}{e}\right)$, il vient (cf. théorème 2, § 3) :

Proposition B_2'.- Soit $D = -pp'$ où $p \equiv p' \equiv 1 \pmod 8$ et $\left(\frac{p}{p'}\right) = -1$.
Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $\lambda(pp') = 1$.

d) Cas où $\varepsilon = 1$. g est toujours dans le genre principal.

d_1) Si $\varepsilon' = 1$, $\varepsilon'' = -1$, les caractères des classes ambiguës sont 1 , 1 , 1 et 1 , -1 , -1 . Le lemme 3 montre que :

Proposition B_3'.- Soit $D = -pp'$ où $\left(\frac{p}{p'}\right) = 1$, $p \equiv 1$, $p' \equiv 5 \pmod 8$.

$(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $\left(\frac{p'}{p}\right)_4 = 1$. Sinon $(C_2) = C(4).C(2)$.

d_2) Si $\varepsilon' = \varepsilon'' = -1$. Les lemmes 1, 2, 3 ne s'appliquent pas. Soit m , premier à $2pp'$, le premier coefficient d'une racine carrée de g :

$$m^2 = px^2 + p'y^2 .$$

Supposons, par exemple, y pair : $y = 2z$, z est impair car $p \equiv 5 \pmod 8$. On a :

$\left(\frac{m}{p}\right) = \left(\frac{p'}{p}\right)_4 \left(\frac{y}{p}\right) = -\left(\frac{p'}{p}\right)_4 \left(\frac{p}{z}\right) = -\left(\frac{p'}{p}\right)_4$; $\left(\frac{m}{p'}\right) = \left(\frac{p}{p'}\right)_4 \left(\frac{x}{p'}\right) = \left(\frac{p}{p'}\right)_4$.

Donc $\left(\frac{-1}{m}\right) = -\left(\frac{p'}{p}\right)_4 \left(\frac{p}{p'}\right)_4$, et, comme les caractères des classes ambiguës sont 1 , 1 , 1 et -1 , -1 , 1 , on trouve :

Proposition B_4'.- Soit $D = -pp'$ où $\left(\frac{p}{p'}\right) = 1$, $p \equiv p' \equiv 5 \pmod 8$.

$(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $\left(\frac{p'}{p}\right)_4 \left(\frac{p}{p'}\right) = -1$. Sinon
$(C_2) = C(4).C(2)$.

Corollaire.- Si $p \equiv p' \equiv 5 \pmod 8$, $\left(\frac{p}{p'}\right) = 1$, $\left(\frac{p'}{p}\right)_4 = \left(\frac{p}{p'}\right)_4 = 1$, $(C_2)\ (pp') = C(\geqslant 8)$, mais $(C_2)\ (-pp') = C(4).C(2)$ ne contient pas de cycles d'ordre au moins 8 .

Exemples : $pp' = 505$, 689 , 793 , 905 , ...

e) Si $\varepsilon = \varepsilon' = \varepsilon'' = 1$, c'est-à-dire si $\left(\frac{p}{p'}\right) = 1$, $p \equiv p' \equiv 1 \pmod 8$, toutes les classes ambiguës sont dans le genre principal, donc $(C_2) = C(\geqslant 4).C(\geqslant 4)$. D'autre part, on peut faire le tableau des caractères des racines carrées de g , h , k : on pose $pp' = 2e^2 - d^2$ $(e > 0)$ et :

$$\alpha = \left(\frac{pp'}{2}\right)_4 \left(\frac{2p}{p'}\right)_4 \left(\frac{2p'}{p}\right)_4 = \left(\frac{aa'+bb'}{p}\right) \left(\frac{2}{a+b}\right) \left(\frac{2}{a'+b'}\right) .$$

	$\sqrt{g}$	$\sqrt{h}$	$\sqrt{k}$
$\left(\frac{m}{p}\right)$	$\left(\frac{p'}{p}\right)_4$	$\left(\frac{e}{p}\right)$	$\left(\frac{p'}{p}\right)_4 \left(\frac{e}{p}\right)$
$\left(\frac{m}{p'}\right)$	$\left(\frac{p}{p'}\right)_4$	$\left(\frac{e}{p'}\right)$	$\left(\frac{p}{p'}\right)_4 \left(\frac{e}{p'}\right)$
$\left(\frac{-1}{m}\right)$	$\left(\frac{p}{p'}\right)_4 \left(\frac{p'}{p}\right)_4$	$\left(\frac{-1}{e}\right)$	α

On en déduit les résultats suivants :

Proposition C_1'.- Soit $D = -pp'$ où $p \equiv p' \equiv 1 \pmod 8$ et $\left(\frac{p}{p'}\right) = 1$.

On a $pp' = 2e^2 - d^2$ et :

$(C_2) = C(\geqslant 8).C(\geqslant 8)$ si, et seulement si, $\left(\frac{p}{p'}\right)_4 = \left(\frac{p'}{p}\right)_4 = \left(\frac{e}{p}\right) = \left(\frac{e}{p'}\right) = 1$.

$(C_2) = C(\geqslant 8).C(4)$ dans les cas suivants :

$\left(\frac{p'}{p}\right)_4 = \left(\frac{p}{p'}\right)_4 = 1$, $\left(\frac{e}{p}\right)$ ou $\left(\frac{e}{p'}\right) = -1$; $\left(\frac{e}{p}\right) = \left(\frac{e}{p'}\right) = 1$, $\left(\frac{p}{p'}\right)_4$ ou $\left(\frac{p'}{p}\right)_4 = -1$; $\left(\frac{p'}{p}\right)_4 = \left(\frac{e}{p}\right)$ et $\left(\frac{p}{p'}\right)_4 = \left(\frac{p}{p'}\right)$, un au moins de ces nombres valant -1 . Dans les autres cas, $(C_2) = C(4).C(4)$.

Exemple : $D = -6497 = -73.89$, où $(C_2) = C(8).C(8)$: c'est la plus petite valeur de $|D|$ telle que (C_2) contienne $C(8)^2$ (cf. [1], p. 43).

Vérifions que $\left(\frac{p}{p'}\right)_4 = \left(\frac{p'}{p}\right)_4 = \left(\frac{e}{p}\right) = \left(\frac{e}{p'}\right) = 1$

$$\left(\frac{89}{73}\right)_4 = \left(\frac{16}{73}\right)_4 = 1 \quad \text{et} \quad \begin{cases} 73 = 3^2 + 8^2 \\ \\ 89 = 5^2 + 8^2 \end{cases} , \text{ donc } \left(\frac{73}{89}\right)_4 = \left(\frac{15+64}{73}\right) = \left(\frac{6}{73}\right) = 1 .$$

On trouve aussi : $73 = 2.7^2 - 5^2$ et : $89 = 2.7^2 - 3^2$. Donc, on voit que :

$$e = 2.49 + 15 + 21 + 35 = 169 = 13^2 \quad \text{et} \quad \left(\frac{e}{p}\right) = \left(\frac{e}{p'}\right) = 1 .$$

Cas 2) : $D = -2pp'$. Les caractères génériques sont $\left(\frac{m}{p}\right)$, $\left(\frac{m}{p'}\right)$, $\left(\frac{-2}{m}\right)$.

Les formes ambiguës simples sont équivalentes à :

$$f = [1,0,2pp'] \ , \ g = [2,0,pp'] \ , \ h = [p,0,2p'] \ , \ k' = [p',0,2p] .$$

Posons $(\frac{p}{p'}) = \varepsilon$, $(\frac{2}{p}) = \varepsilon'$, $(\frac{2}{p'}) = \varepsilon'$

	f	g	h	k'
$(\frac{m}{p})$	1	ε'	$\varepsilon\varepsilon'$	ε
$(\frac{m}{p'})$	1	ε''	ε	$\varepsilon\varepsilon''$
$(\frac{-2}{m})$	1	$\varepsilon'\varepsilon''$	ε'	ε''

a) Si deux ou trois des ε valent -1 , seule f est dans le genre principal, donc $(C_2) = C(2)^2$.

b) Si $\varepsilon' = \varepsilon'' = 1$, $\varepsilon = -1$, g est dans le genre principal. Soit $pp' = e'^2 - 2d'^2$. $(e' > 0)$. On voit que $[e',2d',2e'] = g$, donc comme $\chi(pp') = (\frac{-2}{e'})$, il vient (cf. théorème 2, § 3) :

Proposition B'_5.- Soit $D = -2pp'$ où $p \equiv p' \equiv 1 \pmod 8$ et $(\frac{p}{p'}) = -1$. Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $\chi(pp') = 1$.

c) Si $\varepsilon = \varepsilon' = 1$ et $\varepsilon'' = -1$, h est dans le genre principal et le lemme 3 montre que :

Proposition B'_6.- Soit $D = 2pp'$ où $p \equiv 1$, $p' \equiv 5 \pmod 8$ et $(\frac{p}{p'}) = 1$. Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{2p'}{p})_4 = 1$.

Exemple : $D = -410$: $p' = 5$, $p = 41$ et $(\frac{p}{p'}) = 1$.

$(\frac{2p'}{p})_4 = (\frac{10}{41})_4 = (\frac{2}{41})_4 (\frac{5}{41})_4 = -(\frac{5+2.4}{5}) = 1$. Donc $(C_2) = C(\geqslant 8).C(2)$.

d) Si $\varepsilon = \varepsilon' = \varepsilon'' = 1$, g , h , k sont dans le genre principal et le tableau des caractères de leurs racines carrées contient :

	$\sqrt{g}$	$\sqrt{h}$	$\sqrt{k}$
$(\frac{m}{p})$	$(\frac{e'}{p})$	$(\frac{2p'}{p})_4$	
$(\frac{m}{p'})$	$(\frac{e'}{p'})$		$(\frac{2p}{p'})_4$
$(\frac{-2}{m})$:	$(\frac{-2}{e'})$		

Le tableau se remplit en remarquant que le produit des termes d'une ligne ou d'une colonne vaut 1 . En particulier :

Proposition C'_2.- Soit $D = 2pp'$ où $p \equiv p' \equiv 1 \pmod 8$ et $(\frac{p}{p'}) = 1$. Alors $pp' = e'^2 - 2d'^2$ et $(C_2) = C(\geqslant 8).C(\geqslant 8)$ si, et seulement si, $(\frac{e'}{p'}) = (\frac{e'}{p}) = (\frac{2p'}{p})_4 = (\frac{2p}{p'})_4 = 1$.

Cas 3) : $D = -qpp'$: Les caractères génériques sont $(\frac{m}{p})$, $(\frac{m}{p'})$, $(\frac{m}{q})$.

Les formes ambiguës simples sont :

$$f = [1,0,pp'q] \text{ , } g = [q,0,pp'] \text{ , } h = [p,0,p'q] \text{ , } h' = [p',0,pq] .$$

Posons $\varepsilon = (\frac{p}{p'})$, $\varepsilon' = (\frac{p}{q})$, $\varepsilon'' = (\frac{p'}{q})$. Le tableau des caractères est

	f	g	h	h'
$(\frac{m}{p})$	1	ε'	$\varepsilon\varepsilon'$	ε
$(\frac{m}{p'})$	1	ε''	ε	$\varepsilon\varepsilon''$
$(\frac{m}{q})$	1	$\varepsilon'\varepsilon''$	ε'	ε''

a) Si deux ou trois des ε valent -1 , $(C_2) = C(2)^2$.

b) Si $\varepsilon' = \varepsilon'' = 1$, $\varepsilon = -1$, g est dans le genre principal et les caractères des classes ambiguës sont 1 , 1 , 1 et -1 , -1 , 1 , donc, appliquant le lemme 1, il vient :

Proposition B_7'.- Soit $D = -qpp'$ où $(\frac{p}{q}) = (\frac{p}{q'}) = -(\frac{p}{p'}) = 1$. Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{-q}{pp'})_4 = 1$. Sinon $(C_2) = C(4).C(2)$.

c) Si $\varepsilon = \varepsilon' = 1$ et $\varepsilon'' = -1$, h est dans le genre principal et :

Proposition B_8'.- Soit $D = -qpp'$ où $(\frac{p}{q}) = -(\frac{p'}{q}) = (\frac{p}{p'}) = 1$. Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{-qp'}{p})_4 = 1$. Sinon $(C_2) = C(4).C(2)$.

Exemple : $D = -663 = -3.13.17$: $p = 13$, $p' = 17$, $q = 3$.
On a $(\frac{-51}{13})_4 = 1$, donc $(C_2) = C(\geqslant 8).C(2)$.

d) Si $\varepsilon = \varepsilon' = \varepsilon'' = 1$; le tableau des caractères des racines carrées de g , h , h' est :

	$\sqrt{g}$	$\sqrt{h}$	$\sqrt{h'}$
$(\frac{m}{p})$		$(\frac{-qp'}{p})_4 = \beta$	
$(\frac{m}{p'})$			$(\frac{-pq}{p'})_4 = \gamma$
$(\frac{m}{q})$	$(\frac{-q}{pp'})_4 = \alpha$		

On peut en déduire les résultats suivants :

Proposition C_3'.- Soit $D = -qpp'$ où $(\frac{p}{q}) = (\frac{p}{q'}) = (\frac{p}{p'}) = 1$

Si $(C_2) = C(\geqslant 8).C(\geqslant 8)$, $\alpha = \beta = \gamma = 1$. Inversement :

Si $\alpha = \beta = \gamma = 1$, $(C_2) = C(\geqslant 8).C(\geqslant 8)$ ou $C(4).C(4)$.
Si $\alpha = \beta = \gamma = -1$, $(C_2) = C(4).C(4)$.
Si deux des α , β , γ valent 1 et le troisième -1 , $(C_2) = C(\geqslant 8).C(4)$.
Si un des α , β , γ vaut 1 et les autres -1 , $(C_2) = C(\geqslant 4).C(4)$.

On a : $\alpha\beta\gamma = (\frac{p}{p'})_4 (\frac{p'}{p})_4$.

Cas 4) : $D = -2pq$. Posons $(\frac{p}{q}) = \varepsilon$, $(\frac{2}{p}) = \varepsilon'$, $(\frac{2}{q}) = \varepsilon''$, $p = a^2 + b^2$.

Les caractères génériques sont $(\frac{m}{p})$, $(\frac{m}{q})$, $(\frac{2}{m})$ et les formes ambiguës simples :

$$f = [1,0,2pq] \text{ , } g = [2,0,pq] \text{ , } h = [p,0,2q] \text{ , } k = [q,0,2p] \text{ .}$$

Le tableau de leurs genres est :

	f	g	h	k
$(\frac{m}{p})$	1	ε'	$\varepsilon\varepsilon'$	ε
$(\frac{m}{q})$	1	ε''	ε	$\varepsilon\varepsilon''$
$(\frac{2}{m})$	1	$\varepsilon'\varepsilon''$	ε'	ε''

a) Si deux ou trois des ε valent -1 , $(C_2) = C(2)^2$.

b) Si $\varepsilon' = \varepsilon'' = 1$, $\varepsilon = -1$, c'est-à-dire si $p - q \equiv 1 \pmod 8$ et $(\frac{p}{q}) = -1$.
Alors g est dans le genre principal et $-pq \equiv 1 \pmod 8$ et le lemme 2 montre que :

Proposition B'_9.- Soit $D = -2pq$ où $p \equiv -q \equiv 1 \pmod 8$ et $(\frac{p}{q}) = -1$. Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $p \equiv -q \pmod{16}$. Sinon $(C_2) = C(4).C(2)$.

c) Si $\varepsilon = \varepsilon' = 1$ et $\varepsilon'' = -1$, la forme h est dans le genre principal et $V = p$, donc le lemme 3 donne :

Proposition B'_{10}.- Soit $D = -2pq$ où $p \equiv 1$, $q \equiv 3 \pmod 8$ et $(\frac{p}{q}) = 1$. Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{2q}{p})_4 = 1$. Sinon $(C_2) = C(4).C(2)$.

d) Si $\varepsilon = \varepsilon'' = 1$ et $\varepsilon' = -1$, la forme $k = [2p,0,q]$ est dans le genre principal. Comme $-q \equiv 1 \pmod 8$ et comme $V = q$ ou $2p$, le lemme 2 montre que $e_q(\sqrt{k}) = e_{2p}(\sqrt{k}) = (\frac{-q}{2p})_4$, donc :

Proposition B'_{11}.- Soit $D = -2pq$ où $p \equiv 5$, $q \equiv -1 \pmod 8$ et $(\frac{p}{q}) = 1$. Alors $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{-q}{2p})_4 = 1$. Sinon $(C_2) = C(4).C(2)$.

e) Si $\varepsilon = \varepsilon' = \varepsilon'' = 1$, c'est-à-dire si $(\frac{p}{q}) = 1$, $p \equiv -q \equiv 1 \pmod 8$: g , h et k sont dans le genre principal et le tableau des caractères de leurs racines carrées est : (on a posé $pq = e'^2 - 2d'^2$, donc $[e',2d',2e']^2 = g$)

	$\sqrt{g}$	$\sqrt{h}$	$\sqrt{k}$
$(\frac{m}{p})$	$(\frac{e'}{p})$	$(\frac{2q}{p})_4 = \beta$	
$(\frac{m}{q})$	$(\frac{e'}{q})$		$(\frac{-q}{2p})_4 = \gamma$
$(\frac{2}{m})$	$(\frac{-pq}{2})_4 = \alpha$		

$(\frac{e}{p})$ $(\frac{e'}{q}) = \alpha$ et $\alpha\beta\gamma = \lambda(p) = (\frac{2}{a+b})$. Donc :

Proposition C'_3.- Soit $D = -2pq$ où $p \equiv -q \equiv 1 \pmod 8$ et $(\frac{p}{q}) = 1$.

a) $(C_2) = C(\geqslant 8).C(\geqslant 8)$ si, et seulement si, $\alpha = \beta = \gamma = (\frac{e'}{p}) = 1$.

Si $\alpha = \beta = \gamma = 1$, $(\frac{e'}{p}) = (\frac{e'}{q}) = -1$, alors $(C_2) = C(4).C(4)$.

b) Si un seul des nombres α , β , γ vaut -1 , $(C_2) = C(\geqslant 8).C(4)$.

c) Si deux ou trois des α , β , γ valent -1 , $(C_2) = C(4).C(4)$.

Exemple : $D = -7966 = -2pq$ avec $p = 569$, $q = 7$, $pq = 3983$

$$(\frac{p}{q}) = 1 \ , \ p \equiv -q \equiv 1 \pmod 8 \ , \ p = a^2 + b^2 = 13^2 + 20^2$$

$$\alpha = (\frac{-3983}{2})_4 = 1 \ , \text{ car } 3983 \equiv 783 \equiv 63 \equiv -1 \pmod{16}$$

$$\beta = (\frac{14}{p})_4 = (\frac{2}{p})_4 \, (\frac{7}{p})_4 = -1 \times -1 = 1 \ , \text{ car } 8 \nmid b \ , \ 7 \nmid a \ , \ 7 \nmid b$$

$$\gamma = \lambda(p).\alpha.\beta = 1 \ , \text{ car } \lambda(p) = (\frac{2}{33}) = 1$$

$7 = 2.2^2 - 1$ et $569 = 2.17^2 - 1$, donc $e' = 2.17.2 + 1 = 65$ et $(\frac{65}{7}) = (\frac{2}{7}) = 1$.

Donc : (C_2) $(-7966) = C(8).C(8)$ (cf. [1], p. 43).

Cas 5) : $D = -qq'$. On suppose $(\frac{q}{q'}) = -(\frac{q'}{q}) = 1$ et on pose $\varepsilon = (\frac{2}{q})$, $\varepsilon' = (\frac{2}{q'})$.

Les caractères génériques sont $(\frac{m}{q})$, $(\frac{m}{q'})$, $(\frac{-1}{m})$ et les formes ambiguës simples sont équivalentes à :

$$f = [1,0,qq'] \ , \ g = [q,0,q'] \ , \ h = \left[2,1,\frac{qq'+1}{2}\right] \ , \ k = \left[2q,q,\frac{q+q'}{2}\right] .$$

Leur tableau des caractères est

	f	g	h	k
$(\frac{m}{q})$	1	−1	ε	$-\varepsilon$
$(\frac{m}{q'})$	1	1	ε'	ε'
$(\frac{-1}{m})$	1	−1	$\varepsilon\varepsilon'$	$-\varepsilon\varepsilon'$

a) Si $\varepsilon' = -1$, c'est-à-dire si $q' \equiv 3 \pmod 8$, $(C_2) = C(2)^2$.

b) Si $\varepsilon' = \varepsilon = 1$, c'est-à-dire si $q \equiv q' \equiv -1 \pmod 8$, h est dans le genre principal. Soit $qq' = 2e^2 - d^2$. On voit que $[e,d,2e]^2 = h$ et comme les caractères des classes ambiguës sont 1 , 1 , 1 et −1 , 1 , −1 , on trouve :

Proposition B_{12}.- Soit $D = -qq'$ où $(\frac{q}{q'}) = 1$ et $q \equiv q' \equiv -1 \pmod 8$. Alors $qq' = 2e^2 - d^2$ et $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{e}{q'}) = 1$. Sinon $(C_2) = C(4).C(2)$.

c) Si $\varepsilon' = 1$, $\varepsilon = -1$, c'est-à-dire si $q' \equiv -1$, $q \equiv 3 \pmod 8$, k est dans le genre principal. Donc $(C_2) = C(\geqslant 4).C(2)$.

Les méthodes que nous utilisons ne permettent pas d'obtenir des informations sur les racines carrées de k , donc, nous ne pouvons pas, ici, trouver de critère pour que (C_2) ait une composante d'ordre $\geqslant 8$.

Cas 6) : $D = -qq'q''$. Les caractères génériques sont $(\frac{m}{q})$, $(\frac{m}{q'})$, $(\frac{m}{q''})$.

Les formes ambiguës simples sont :

$$f = [1,0,qq'q"] \ , \ g = [q,0,q'q"] \ , \ g' = [q',0,qq"] \ , \ g" = [q",0,qq'] \ .$$

Posons $\varepsilon = (\frac{q'}{q"})$, $\varepsilon' = (\frac{q"}{q})$, $\varepsilon" = (\frac{q}{q'})$:

	f	g	g'	g"
$(\frac{m}{q})$	1	$-\varepsilon'\varepsilon"$	$-\varepsilon"$	ε'
$(\frac{m}{q'})$	1	$\varepsilon"$	$-\varepsilon\varepsilon"$	$-\varepsilon$
$(\frac{m}{q"})$	1	$-\varepsilon'$	ε	$-\varepsilon\varepsilon'$

On voit que, par exemple, g est dans le genre principal, si, et seulement si, $\varepsilon" = -\varepsilon' = 1$, c'est-à-dire, si, et seulement si, $(\frac{q}{q'}) = (\frac{q}{q"}) = 1$ et alors, g' et g" ne sont pas dans le genre principal. Donc :
$(C_2) = C(\geqslant 4).C(2)$ <u>si, et seulement si</u>, $\varepsilon" = -\varepsilon' = 1$ <u>ou</u> $\varepsilon = -\varepsilon" = 1$ <u>ou</u> $\varepsilon' = -\varepsilon = 1$. <u>Sinon</u> $(C_2) = C(2).C(2)$.

Supposons, par exemple, $(\frac{q}{q'}) = (\frac{q}{q"}) = 1$. Considérons $g = [q,0,q'q"]$ et posons $N = q$ et $M = q'q"$ dans le lemme 8.

Il existe des entiers X , Y , k , ℓ et m tels que :

$$q'q" = k^2 X^2 + 2\ell XY + 2m Y^2 \ ; \ q = \ell^2 - 2k^2 m \ .$$

Supposons $(\frac{q'}{q"}) = \varepsilon = 1$. Les caractères des classes ambiguës sont 1 , 1 , 1 et -1 , -1 , 1 , donc $V = q"$. On trouve donc, en posant $A' = |A| = |k^2 X - \ell Y|$ si A est impair (Y pair) ou $A' = \frac{|A|}{2}$ si A est pair :

<u>Proposition</u> B'_{13}.- <u>Soit</u> $D = -qq'q"$ <u>où</u> $(\frac{q}{q'}) = (\frac{q}{q"}) = (\frac{q'}{q"}) = 1$. <u>Alors</u> $(C_2) = C(\geqslant 8).C(2)$ <u>si, et seulement si</u>, $(\frac{A'}{q"}) = 1$. <u>Sinon</u> $(C_2) = C(4).C(2)$.

<u>Cas particulier</u> : Si il y a deux classes de déterminant -q , alors :
$q'q" = x^2 - qy^2 = (X+Y)^2 - qY^2 = X^2 + 2XY + (q-1)Y^2$, où $y = Y$, $x = X + Y$, $A = X + Y = x$, donc, posant $x' = |x|$ si x est impair, $x' = \frac{|x|}{2}$ si x est pair, $(C_2) = C(\geqslant 8).C(2)$ <u>si, et seulement si</u>, $(\frac{x'}{q"}) = 1$. <u>Sinon</u> $(C_2) = C(4).C(2)$

<u>Exemple</u> : $D = -3.11.23 = -759$; $(C_2) = C(4).C(2)$. En effet :

$(\frac{3}{11}) = (\frac{3}{23}) = 1$, donc $q = 3$; $(\frac{23}{11}) = 1$, donc $q" = 11$.

$11.23 = 253 = 256 - 3$, donc $x = 16$, $x' = 8$ et $(\frac{8}{11}) = -1$.

<u>Exemple</u> : $D = -903 = -3.7.43$; $(C_2) = C(8).C(4)$. En effet :

$(\frac{43}{7}) = (\frac{43}{3}) = 1$, $q = 43$; $(\frac{7}{3}) = 1$, $q" = 3$; $h(43) = 2$

$21 = 8^2 - 43$, donc $x = 8$, $x' = 4$ et on a bien $(\frac{x'}{q"}) = (\frac{4}{3}) = 1$.

On peut aussi déterminer les caractères d'une racine carrée de g d'une autre manière. Posons $q'q" = P$; si $g = [q,0,P]$ est dans le genre principal, P est représenté par une forme φ du genre principal de déterminant q . Comme

$(C_2)(q) \neq C(2)$, l'ordre de φ est impair, donc aussi le plus petit entier P tel que $P = X^2 - qY^2$ avec $(X,Y) = 1$, $X > 0$. Raisonnant comme dans le cas $D = Pqq'$, on trouve que le premier coefficient d'une racine carrée de g est X si X est impair, $2X$ si X est pair.

Cas 7) : $D = -2qq'$. Les caractères génériques sont $(\frac{m}{q})$, $(\frac{m}{q'})$, $(\frac{-2}{m})$

Soit $(\frac{q}{q'}) = -(\frac{q'}{q}) = 1$, $\varepsilon = (\frac{2}{q})$, $\varepsilon' = (\frac{2}{q'})$

Les formes ambiguës simples et leurs caractères sont :

$$f = [1,0,2qq'] \ , \ g = [2,0,qq'] \ , \ h = [q,0,2q'] \ , \ h' = [q',0,2q] .$$

	f	g	h	h'
$(\frac{m}{q})$	1	ε	$-\varepsilon$	-1
$(\frac{m}{q'})$	1	ε'	1	ε'
$(\frac{-2}{m})$	1	$\varepsilon\varepsilon'$	$-\varepsilon$	$-\varepsilon'$

a) Si $\varepsilon = 1$, $\varepsilon' = -1$, c'est-à-dire si $q \equiv -1$, $q' \equiv 3 \pmod 4$, $(C_2) = C(2).C(2)$. Sinon $(C_2) = C(\geqslant 4).C(2)$.

b) Si $\varepsilon = \varepsilon' = +1$, c'est-à-dire si $q \equiv q' \equiv -1 \pmod 8$, g est dans le genre principal et $qq' = e'^2 - 2d'^2$, donc $[e',2d',2e']^2 = g$, donc, on trouve

Proposition B'_{14}.- Soit $D = -2qq'$ où $q \equiv q' \equiv -1 \pmod 8$. Alors $qq' = e'^2 - 2d'^2$ et $(C_2) = C(\geqslant 8).C(2)$, si, et seulement si, $(\frac{e'}{q'}) = 1$. Sinon $(C_2) = C(4).C(2)$.

c) Si $\varepsilon = -1$, c'est-à-dire si $q \equiv 3 \pmod 8$, h est dans le genre principal. Posons $N = q$, $M = 2q'$ dans le lemme 8. Il existe des entiers X , Y , k , ℓ et m tels que :

$$2q' = k^2 X^2 + 2\ell XY + 2m Y^2 \ ; \ q = \ell^2 - 2k^2 m .$$

Le nombre $A = k^2 X + \ell Y$ est impair. On obtient donc :

Proposition B'_{15}.- Soit $D = -2qq'$ tel que $(\frac{q}{q'}) = 1$ et $q \equiv 3 \pmod 8$.
Si $q' \equiv 3 \pmod 8$, $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{-2}{|X+\ell Y|}) = 1$.
Si $q' \equiv -1 \pmod 8$, $(C_2) = C(\geqslant 8).C(2)$ si, et seulement si, $(\frac{|k^2X+Y|}{q'}) = 1$.

Si il y a deux classes de déterminant $-q$, on a $2q' = x^2 - qy^2$, où x et y sont impairs et on trouve que l'on peut remplacer $|A|$ par $|x|$ dans la proposition B'_{15}.

§ 12.- Etude de certains cas où $D < 0$ et (C_2) est produit de plus de deux groupes cycliques.

1) Soit $P = p_1 \dots p_n$ où $p_i \equiv 1 \pmod 8$ $(i = 1, \dots, n)$. Comme au § 3, posons : $P = a^2 + b^2 = u^2 + 2v^2 = 2e^2 - d^2 = e'^2 - 2d'^2$ (a impair, e et e' positifs) et aussi (cf. § 3, théorème 2) :

$$\lambda(P) = \left(\frac{2}{a+b}\right) = (-1)^{\frac{v}{2}} = \left(\frac{-1}{e}\right) \quad ; \quad \mu(P) = \left(\frac{2}{a}\right) = \left(\frac{2}{d}\right) = \left(\frac{P}{2}\right)_4$$

$$\nu(P) = \left(\frac{2}{u}\right) = (-1)^{\frac{b}{4}} = \left(\frac{-2}{e'}\right) = \left(\frac{2}{P}\right)_4 .$$

Nous supposerons que $\left(\frac{p_i}{p_j}\right) = -1$ $(1 \leqslant i < j \leqslant n)$ et que n est 2 ou un nombre impair.

a) Cas de $D = -P$.

Les formes ambiguës simples du genre principal sont $f = [1,0,P]$ et $h = \left[2,1,\frac{1+P}{2}\right]$. Une classe ambiguë contient soit une forme $g_1 = [P_1,0,P_2]$, soit une forme $k_1 = \left[2P_1,P_1,\frac{P_1+P_2}{2}\right]$, avec $P_1 P_2 = P$. Comme $P_1 \equiv P_2 \equiv 1 \pmod 8$, $P_1 \equiv \frac{P_1 + P_2}{2} \equiv 1 \pmod 4$, donc pour toute classe ambiguë e_2 vaut 1 , donc $V = 2$. Comme une racine carrée de h est $[e,d,2e]$, on obtient par la méthode B :

Proposition B'_{16}.- Soit $D = -p_1 \dots p_n = -P$ où $p_i \equiv 1 \pmod 8$ $(i = 1, \dots, n)$, $\left(\frac{p_i}{p_j}\right) = -1$ $(1 \leqslant i < j \leqslant n)$ et où n est 2 ou un nombre impair. Alors $(C_2) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $\lambda(P) = 1$. Sinon $(C_2) = C(4).C(2)^{n-1}$.

b) Cas de $D = -2P$.

Les formes ambiguës simples du genre principal sont $f = [1,0,2P]$ et $h = [2,0,P]$ et toute forme ambiguë simple $g_1 = [P_1,0,2P_2]$ $(P_1 P_2 = P)$ vérifie $e_2(g_1) = \left(\frac{-2}{P_1}\right) = 1$, donc $V = 2$. Ici, une racine carrée de h est $[e',2d',2e']$, donc :

Proposition B'_{17}.- Soit $D = -2p_1 \dots p_n = -2P$ où les p_i vérifient les hypothèses de la proposition B'_{16}. Alors $(C_2) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $\nu(P) = 1$. Sinon $(C_2) = C(4).C(2)^{n-1}$.

Corollaire.- (C_2) $(2P)$ contient une composante d'ordre $\geqslant 8$ si, et seulement si. (C_2) $(-P)$ et (C_2) $(-2P)$ en contiennent.

2) Soit $D = -qP$, où $P = p_1 \dots p_n$ avec n = 2 ou un nombre impair, $\left(\frac{p_i}{p_j}\right) = -1$, $\left(\frac{q}{p_i}\right) = 1$.

Les formes ambiguës simples du genre principal sont $f = [1,0,Pq]$ et $g = [P,0,q]$. Une forme ambiguë simple est $h = [qP',0,P'']$ avec $P'P'' = P$,

donc la forme h vérifie $e_q(h) = e_P(h) = 1$, donc $V = P$ et appliquant le lemme 1 :

Proposition B'_{18}.- Soit $D = -qp_1 \ldots p_n = -qP$, où $(\frac{q}{p_i}) = 1$, $(\frac{p_i}{p_j}) = -1$ $(1 \leqslant i < j \leqslant n)$ et où n est 2 ou un nombre impair.

Alors $(C_2) = C(\geqslant 8).C(2)^{n-1}$ si, et seulement si, $(\frac{-q}{p})_4 = 1$. Sinon $(C_2) = C(4).C(2)^{n-1}$.

Les propositions B'_2, B'_5 et B'_7 sont le cas $n = 2$ des propositions B'_{16}, B'_{17} et B'_{18} respectivement.

Le seul résultat du travail [11] qui ne soit pas un cas particulier des résultats des paragraphes 3 et 12 est le suivant : ([11], théorème 4)

Soit $D = -2q$ où $q \equiv -1 \pmod 8$. Alors $(C_2) = C(\geqslant 8)$ si, et seulement si, $q \equiv -1 \pmod{16}$. Sinon $(C_2) = C(4)$.

Les propositions B'_3, B'_4 et B'_{17} étaient connues de Redei [15].

Les propositions B'_2, B'_{12} et une partie de la proposition C'_1 se trouvent dans le travail [5] de E. Brown.

§ 13.- Représentation de nombres premiers par des formes quadratiques binaires de déterminant $-\pi$, où $\pi \equiv 1 \pmod 4$.

Rappelons que un nombre premier p, premier à D, ne peut être représenté que par deux classes inverses K et K^{-1} de formes quadratiques binaires proprement primitives de déterminant donné D. Le but essentiel de ce paragraphe est de démontrer le résultat suivant :

Théorème 3.- Soit $\pi \equiv 1 \pmod 8$ un nombre premier et soit p un autre nombre premier représenté par les classes K et K^{-1} du genre principal de déterminant $-\pi$, c'est-à-dire tel que $\left(\frac{p}{\pi}\right) = (-1)^{\frac{p-1}{2}} = 1$.

Les classes K et K^{-1} sont des puissances quatrièmes si, et seulement si,

$$\left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = 1 .$$

La démonstration consiste à combiner une méthode de Dirichlet, analogue à celle des lemmes 1 à 3, avec la théorie de la composition des formes quadratiques binaires :

Proposition 2 (Dirichlet [6], pages 202-209, si $\pi \equiv 1 \pmod 8$).- Soit $\pi \equiv 1 \pmod 4$ un nombre premier, $P \equiv 1 \pmod 4$ un nombre premier à π, tels que $P = t^2 + \pi u^2$ et $(t,u) = 1$. Alors :

$$(1) \qquad \left(\frac{tu}{P}\right) = (-1)^{\frac{P-1}{4} + u\frac{\pi-1}{4}} \left(\frac{t}{\pi}\right) .$$

1) Si t est impair, $u = 2^h u'$. On voit que $h = 1$ si $P \equiv 5 \pmod 8$ et :

$$\left(\frac{t}{P}\right) = \left(\frac{P}{t}\right) = \left(\frac{\pi}{t}\right) = \left(\frac{t}{\pi}\right) ; \quad 1 = \left(\frac{P}{u'}\right) = \left(\frac{u'}{P}\right) = \left(\frac{u}{P}\right)\left(\frac{2^h}{P}\right) = \left(\frac{u}{P}\right)(-1)^{\frac{P-1}{4}} .$$

La formule (1) est donc vraie si u est pair.

2) Si t est pair, $t = 2^k t'$, u est impair.

$$\left(\frac{2}{P}\right)^k \left(\frac{t}{P}\right) = \left(\frac{t'}{P}\right)^{\bullet} = \left(\frac{P}{t'}\right) = \left(\frac{\pi}{t'}\right) = \left(\frac{t'}{P}\right) = \left(\frac{2}{\pi}\right)^k \left(\frac{t}{\pi}\right) ; \quad 1 = \left(\frac{P}{u}\right) = \left(\frac{u}{P}\right) .$$

Multipliant : $\left(\frac{tu}{P}\right) = \left(\frac{t}{\pi}\right)\left(\frac{2}{P\pi}\right)^k = \left(\frac{t}{\pi}\right)\left(\frac{2}{P\pi}\right)$, car $k = 1$ si $\left(\frac{2}{P\pi}\right) = -1$

La formule (1) est donc vraie si u est impair. C. Q. F. D.

Soit p un nombre premier tel que $\left(\frac{p}{\pi}\right) = (-1)^{\frac{p-1}{2}} = 1$; p est représenté par les classes K et K^{-1} de déterminant $-\pi$. Les classes K et K^{-1} sont dans le genre principal, donc des carrées. Soit m, choisi premier à $2p\pi$, le premier coefficient d'une forme appartenant à une racine carrée de K ou K^{-1} :

$$(2) \qquad pm^2 = t^2 + \pi u^2 .$$

Appliquons la proposition 2 avec $P = pm^2 \equiv p \pmod 8$:

$$\left(\frac{tu}{p}\right) = \left(\frac{tu}{P}\right) = (-1)^{\frac{P-1}{4} + u\frac{\pi-1}{4}} \left(\frac{t}{\pi}\right) = (-1)^{\frac{p-1}{4} + u\frac{\pi-1}{4}} \left(\frac{t}{\pi}\right) .$$

La relation (2) montre que : $\left(\frac{tu}{p}\right) = (-1)^{\frac{p-1}{4}} \left(\frac{\pi}{p}\right)_4$; $\left(\frac{t}{\pi}\right) = \left(\frac{m}{\pi}\right) \left(\frac{p}{\pi}\right)_4$.

Donc le caractère $\left(\frac{m}{\pi}\right)$ d'une racine carrée $\mathfrak{L}$ de K vérifie :

$$(3) \qquad \left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = \left(\frac{m}{\pi}\right) (-1)^{u\frac{\pi-1}{4}} .$$

a) Cas où $\pi \equiv 1 \pmod 8$.

L'égalité (3) s'écrit : $\left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = \left(\frac{m}{\pi}\right)$. Ceci achève de démontrer le théorème 3.

Corollaire.- Soit $\pi = \alpha^2 + \beta^2 \equiv 1 \pmod 8$. Si $2p$ est représenté par $t^2 + \pi u^2$, alors $\left(\frac{p}{\pi}\right) \left(\frac{\pi}{p}\right)_4 = (-1)^{\frac{h(-\pi)}{4}} = \left(\frac{2}{\alpha+\beta}\right) = \lambda(\pi)$.

En effet, p est alors représenté par la classe $\mathfrak{A}$ de $\left[2,1,\frac{1+\pi}{2}\right]$, qui est la classe ambiguë distincte de $\mathfrak{J}$. La classe $\mathfrak{A}$ est une puissance quatrième si, et seulement si, $h(-\pi) \equiv 0 \pmod 8$.

Cas particuliers :

1) $h(-\pi) = 4$ (Dirichlet [6], page 209).

Le genre principal est formé de $\mathfrak{J}$ et de la classe ambiguë $\mathfrak{A}$. Donc : p est représenté par $f = [1,0,\pi]$ si $\left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = 1$, par $\left[2,1,\frac{1+\pi}{2}\right]$ si $\left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = -1$.

Il est très probable que les seuls π tels que $h(-\pi) = 4$ sont 17 , 73 , 97 , 193 .

2) $h(-\pi) = 8$, c'est-à-dire $(C_2)(-\pi) = C(8)$. Soit $\pi = 2\varepsilon^2 - \delta^2$ $(\varepsilon > 0)$.

Ici, les classes ambiguës $\mathfrak{J}$ et $\mathfrak{A}$ sont des puissances quatrièmes.

Les racines carrées de $\mathfrak{A}$ sont les classes inverses $\mathfrak{B}$ et $\mathfrak{B}'$ contenant respectivement $[\varepsilon,\delta,2\varepsilon]$ et $[\varepsilon,-\delta,2\varepsilon]$. Donc :

Si $\left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = 1$, p est représenté par $\mathfrak{J}$ ou $\mathfrak{A}$.

Si $\left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = -1$, p est représenté par $\mathfrak{B}$ et $\mathfrak{B}'$.

Il est très probable que les seuls π tels que $h(-\pi) = 8$ sont 41 , 113 , 137 , 313 , 337 , 457 et 577 .

3) $h(-\pi) = 16$. On trouve ici, avec les mêmes notations :
$\left(\frac{p}{\pi}\right)_4 \left(\frac{\pi}{p}\right)_4 = 1$ si, et seulement si, p est représenté par $\mathfrak{J}$, $\mathfrak{A}$ ou $\mathfrak{B}$.

Remarque : E. Brown [3] et E. Lehmer [14] ont démontré aussi le corollaire et les cas particuliers 1) et 2), mais, faute de disposer du théorème 3, devaient, pour le cas particulier 2), examiner chacun des cas. L'équation (3) se trouve dans [14], (page 369), mais le nombre m (noté s dans [14]) n'y est pas interprété comme coefficient d'une racine carrée de classe qui représente p .

b) Cas où $q \equiv 5 \pmod 8$.

Alors $h(-q) \equiv 2 \pmod 4$.

Soit p représenté par une classe du genre principal de déterminant $-q$. L'ordre de cette classe est impair. Soit $\omega = 2\mu + 1$ un nombre impair tel que $p^{\omega} = t^2 + q u^2$. Posant $p^{\mu} = m$ dans l'équation (2), on obtient, puisque $\left(\frac{p}{q}\right) = 1$

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^u .$$

Utilisant la théorie pour $D = pq$ (cf. § 3), on obtient :

Proposition 3.- Soit $q \equiv 5 \pmod 8$ et $p \equiv 1 \pmod 8$ tel que $\left(\frac{p}{q}\right) = 1$ et soit $p^{\omega} = t^2 + q u^2$ la plus petite puissance de p représentée par $[1,0,q]$.

a) (C_2) $(pq) = C(\geqslant 8)$ si, et seulement si, $\left(\frac{p}{q}\right)_4 = (-1)^u = 1$.

b) Si $\left(\frac{p}{q}\right)_4 = -1$ $(-1)^u = 1$, $[1,0,-pq]$ représente -1 .

c) Si $\left(\frac{p}{q}\right)_4 = 1$, $(-1)^u = -1$, $[1,0,-pq]$ représente q .

d) Si $\left(\frac{p}{q}\right)_4 = (-1)^u = -1$, $[1,0,-pq]$ représente $-q$.

Une partie de cette proposition a été obtenue par E. Brown [2] et par E. Lehmer [14].

Après avoir obtenu le théorème 3 quand $D = -q$, où $q \equiv 1 \pmod 8$, on peut se demander ce que donne la même méthode dans d'autres cas, en particulier quand (C_2) est cyclique :

A) Cas $D = -2q$ où $q \equiv 1 \pmod 8$.

Soit $P \equiv 1 \pmod 4$ tel que $P = t'^2 + 2q u'^2$. Donc $\left(\frac{P}{q}\right) = 1$, $P \equiv 1 \pmod 8$ et :

$$\left(\frac{t'}{P}\right) = \left(\frac{P}{t'}\right) = \left(\frac{2}{t'}\right) \left(\frac{q}{t'}\right) = \left(\frac{2}{t'}\right) \left(\frac{t'}{q}\right) ; \left(\frac{u'}{P}\right) = \left(\frac{v'}{P}\right) = \left(\frac{P}{v}\right) = 1 .$$

Donc :

$$\left(\frac{t'u'}{P}\right) = \left(\frac{2}{t'}\right) \left(\frac{t'}{q}\right) .$$

Soit maintenant un nombre premier $p \equiv 1 \pmod 8$ tel que $\left(\frac{P}{q}\right) = 1$.

p est représenté par le genre principal de déterminant $-2q$; soit m' , premier à $2q$, représenté par la racine carrée d'une classe représentant p :

$$P = pm'^2 = t'^2 + 2q u'^2 \quad (m' > 0) .$$

On a :

$$\left(\frac{t'}{q}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{m'}{q}\right) ; \left(\frac{2}{t'}\right) = \left(\frac{p}{2}\right)_4 \left(\frac{2}{m'}\right) (-1)^{\frac{u'}{2}} ; \left(\frac{t'u'}{p}\right) = \left(\frac{-2q}{p}\right)_4 = \left(\frac{2q}{p}\right)_4$$

Donc :

$$\left(\frac{2q}{p}\right)_4 = \left(\frac{p}{2}\right)_4 \left(\frac{2}{m'}\right) (-1)^{\frac{u'}{2}} \left(\frac{p}{q}\right)_4 \left(\frac{m'}{q}\right) .$$

La formule du produit : $(\frac{-2}{m'})\ (\frac{m'}{q})=1$ montre que $(\frac{2}{m'})\ (\frac{m'}{q})=(\frac{-1}{m'})$, donc :

$$(4)\qquad (\frac{2q}{p})_4\ (\frac{p}{2q})_4=(\frac{-1}{m'})\ (-1)^{\frac{u'}{2}}\ .$$

B) Cas $D=2q$, où $q\equiv 1\pmod 8$. Raisonnons comme en a) :

Soit $P=pm^2=t''^2-2qu''^2$, où $p\equiv 1\pmod 8$ est tel que $(\frac{p}{q})=1$ et où m, premier à $2q$, est représenté par une racine carrée d'une classe représentant p. Ici, on trouve, en supposant $t''>0$:

$$(\frac{t''}{P})=(\frac{P}{t''})=(\frac{-2}{t''})\ (\frac{q}{t''})=(\frac{-1}{t''})\ (\frac{2}{t''})\ (\frac{t''}{q})\ ;\ (\frac{u''}{P})=(\frac{v''}{P})=(\frac{P}{v''})=1\ .$$

Donc $(\frac{t''u''}{P})=(\frac{-1}{t''})\ (\frac{2}{t''})\ (\frac{t''}{q})$, et, d'autre part :

$$(\frac{2p}{q})_4=(\frac{t''u''}{p})=(\frac{t''u''}{P})\ ;\ (\frac{2}{t''})=(\frac{p}{2})_4\ (\frac{2}{m})\ (-1)^{\frac{u''}{2}}\quad\text{et}\quad(\frac{t''}{q})=(\frac{m''}{q})\ (\frac{p}{q})_4\ .$$

Ici, la formule du produit est $(\frac{2}{m''})\ (\frac{m''}{q})=1$, donc :

$$(5)\qquad (\frac{2p}{q})_4\ (\frac{q}{2p})_4=(\frac{-1}{t''})\ (-1)^{\frac{u''}{2}}\ .$$

Combinant les trois cas $D=-q$, $-2q$, $2q$, on peut énoncer, en se souvenant que, si $p=a^2+b^2\equiv 1\pmod 8$, $\lambda(p)=(\frac{2}{a+b})=(\frac{2}{p})_4\ (\frac{p}{2})_4$:

Proposition 4.- Soient $p\equiv q\equiv 1\pmod 8$ deux nombres premiers tels que $(\frac{p}{q})=1$ et soient m, m', m'', t, u, t', u', t'', u'' des entiers positifs tels que :

a) $(m,2q)=(m',2q)=(m'',2q)=(t,u)=(t',u')=(t'',u'')=1$.

b) $pm^2=t^2+qu^2$; $pm'^2=t'^2+2qu'^2$, $pm''^2=t''^2-2qu''^2$. Alors :

$$(6)\qquad (\frac{p}{q})_4\ (\frac{q}{p})_4=(\frac{m}{q})=(\frac{-1}{m}){}=(\frac{-1}{m'})\ (-1)^{\frac{u'}{2}}\ \lambda(p)=(\frac{-1}{t''})\ (-1)^{\frac{u''}{2}}\ \lambda(p)\ .$$

C) Cas $D=qq'$.

Soient $q\equiv q'\equiv 1\pmod 4$ deux nombres premiers et p un nombre premier $\equiv 1\pmod 4$ tel que $(\frac{p}{q})=(\frac{p}{q'})=1$. p est représenté par le genre principal de déterminant qq', donc si m est représenté par une racine carrée d'une classe représentant p et $(m,2qq')=1$: $pm^2=t^2-qq'u^2$, où $t>0$ est impair et $u=2^h v$ avec $h=1$ si $p\equiv 5\pmod 8$.

$$(\frac{t}{p})=(\frac{p}{t})=(\frac{-qq'u^2}{t})=(\frac{-1}{t})\ (\frac{t}{q})\ (\frac{t}{q'})\ ;\ (\frac{u}{p})=(-1)^{\frac{p-1}{4}}\ (\frac{v}{p})=(-1)^{\frac{p-1}{4}}\ .$$

$$(\frac{t}{q})=(\frac{m}{q})\ (\frac{p}{q})_4\ ;\ (\frac{t}{q'})=(\frac{m}{q'})\ (\frac{p}{q'})_4\ ;\ (\frac{m}{q})\ (\frac{m}{q'})=1\quad\text{(formule du produit)}.$$

Comme $(\frac{tu}{p})=(\frac{-qq'u^2}{p})_4=(-1)^{\frac{p-1}{4}}\ (\frac{qq'u^2}{p})_4$, on trouve ici :

$$(7)\qquad (\frac{p}{qq'})_4\ (\frac{qq'}{p})_4=(\frac{-1}{t})\ .$$

Nous avons ainsi démontré le résultat suivant :

Proposition 4.- Soient q, q' et p trois nombres premiers congrus à 1 modulo 4 et tels que $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = 1$. Il existe des entiers m, t, u tels que $pm^2 = t^2 - qq'u^2$ et que m soit premier à $2qq'$. On a alors :

$$\left(\frac{p}{qq'}\right)_4 \left(\frac{qq'}{p}\right)_4 = \left(\frac{-1}{|t|}\right) .$$

-=oOo=-

Appendice : Correspondance entre le groupe (C) des classes de formes quadratiques binaires de déterminant D et le groupe (C^*) des classes d'idéaux au sens strict de $Q(\sqrt{D})$.

Soit D un entier quadrat-frei. Le discriminant d du corps $Q(\sqrt{D})$ est égal à D si $D \equiv 1 \pmod 4$, à $4D$ si $D \not\equiv 1 \pmod 4$.

Nous noterons $\{a,b,c\}$ la forme quadratique binaire $aX^2 + bXY + cY$ à coefficients entiers. Comme l'ensemble des classes de formes $[A,B,C]$ de déterminant D , l'ensemble des classes de formes $\{a,b,c\}$ telles que $b^2 - 4ac = d$ forme un groupe pour la composition : deux classes L et L' étant données, il existe des couples $\{a,b,a'c\} \in L$ et $\{a',b,ac\} \in L'$; la classe de $\{aa',b,c\}$ ne dépend que de L et L' , est dite composée ou produit de L et L' .

On prouve, d'autre part, le résultat suivant (cf. [10] , pages 210-217, en particulier page 214) :

Il existe une bijection $\mathcal{B}$ entre l'ensemble des classes d'idéaux au sens étroit de $Q(\sqrt{D})$ et les classes de formes $\{a,b,c\}$ telles que $b^2 - 4ac = d$; à la classe de la forme $\{a,b,c\}$ correspond la classe de l'idéal $(a, \frac{b-\sqrt{d}}{2})$.

La bijection $\mathcal{B}$ est un isomorphisme entre les groupes (C_1) et (C^*) . En effet, aux classes de $\{a,b,a'c\}$, $\{a',b,ac\}$ et $\{aa',b,c\}$ correspondent respectivement des classes des idéaux :

$$I = (a, \frac{b-\sqrt{d}}{2}) \quad , \quad I' = (a', \frac{b-\sqrt{d}}{2}) \quad , \quad J = (aa', \frac{b-\sqrt{d}}{2}) \ .$$

On a : $II' = (aa', a'(\frac{b-\sqrt{d}}{2}), a(\frac{b-\sqrt{d}}{2}), (\frac{b-\sqrt{d}}{2})^2) \subset J$.

Si, ce qui est possible, on a choisi a' premier à a , on voit que $J \subset II'$, donc $J = II'$. C. Q. F. D.

a) Cas où $D \equiv 1 \pmod 4$: Ici, $d = 4D$, donc le nombre b est pair, égal à $2B$. Les formes $\{a,b,c\}$ telles que $b^2 - 4ac = d = 4D$ sont les formes $[a,B,c]$ telles que $B^2 - ac = D$. Donc les trois groupes (C) , (C_1) et (C^*) sont isomorphes.

b) Cas où $D \equiv 1 \pmod 4$: Ici, $d = D \equiv 1 \pmod 4$ et le groupe (C_1) est le groupe des formes $\{a,b,c\}$ telles que $b^2 - 4ac = D$; le nombre b est donc impair.

Considérons une classe K de (C) . On voit qu'on peut en choisir des représentants $[A,B,4C']$ où A et B sont impairs et la forme $\{A,B,C'\}$ est dans une classe L de (C_1) déterminée par K . On définit ainsi un homomorphisme de (C) sur (C_1) et on prouve (cf. [7], pages 397-402 ou [13], page 128) que son noyau a un ou trois éléments.

-=oOo=-

BIBLIOGRAPHIE

[1] L. Bouvier, Table des 2-rang, 4-rang et 8-rang du 2-groupe des classes d'idéaux au sens restreint de $Q(\sqrt{m})$, l'Enseignement mathématique 18 (1972), 37-45 et Institut de Mathématiques pures (Grenoble 1971).

[2] E. Brown, Representations of Discriminantal Divisors by Binary Quadratic Forms, J. Number Theory 3 (1971), 213-225.

[3] E. Brown, Quadratic Forms and Biquadratic Reciprocity, J. reine und angew. Math. 253 (1969), 175-184.

[4] E. Brown, Discriminantal Divisors and Binary Quadratic Forms, Glasgow Math. J. 13 (1972), 69-73.

[5] E. Brown, Class Numbers of Complex Quadratic Fields, J. Number Theory, (à paraître).

[6] P. G. L. Dirichlet, Werke I, (Chelsea).

[7] P. G. L. Dirichlet-R. Dedekind, Vorlesungen über Zahlentheorie (Chelsea).

[8] C. F. Gauss, Disquisitiones Arithmeticae.

[9] G. Gras, Problèmes de ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ, thèse, Grenoble (1972), Annales de l'Institut Fourier.

[10] E. Heche, Vorlesungen über die Theorie der Algebraischen Zahlen (Chelsea).

[11] P. Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et réciprocité biquadratique, J. Math. Soc. of Japan 25 (1973).

[12] P. Kaplan, Cycles d'ordre au moins 16 dans le 2-groupe des classes de certains corps quadratiques (à paraître).

[13] P. Kaplan, Cours d'Arithmétique, U. E. R. de Mathématiques, Nancy (1972).

[14] E. Lehmer, On Some Special Quartic Reciprocity Laws, Acta Arithmetica 21 (1972), 367-377.

[15] G. Pall, Discriminantal Divisors of Binary Quadratic Forms, J. Number Theory 1 (1969), 525-533.

[16] L. Redei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. reine und angew. Math. 171 (1934), 131-148.

[17] A. Schölz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Zeitschrift 39 (1935), 95-111.

[18] D. Shanks, Gauss's Ternary Form Reduction and the 2-Sylow Subgroup, Math. of Computation 25 (1971), 837-853.

[19] T. Stieltjes, Contribution à la théorie des résidus cubiques et biquadratiques, Oeuvres, I, 210-275.

[20] F. Tano, Sur quelques théorèmes de Dirichlet, J. reine und angew. Math. 105 (1889), 160-169.

[21] W. C. Waterhouse, Pieces of Eight in Class Groups of Quadratic Fields, J. Number Theory 5 (1973), 95-97.

-=o0o=-